

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2001 年 3 月 15 日 (15.03.2001)

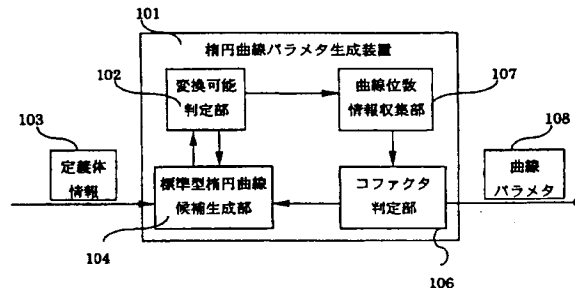
PCT

(10) 国際公開番号
WO 01/18772 A1

- (51) 国際特許分類⁶: G09C 1/00, H04L 9/30 浜市戸塚区戸塚町5030番地 株式会社 日立製作所 ソフトウェア事業部内 Kanagawa (JP).
- (21) 国際出願番号: PCT/JP99/04869
- (22) 国際出願日: 1999 年 9 月 8 日 (08.09.1999)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 桶屋勝幸 (OKEYA, Katsuyuki) [JP/JP]; 〒244-8555 神奈川県横
- (74) 代理人: 弁理士 作田康夫 (SAKUTA, Yasuo); 〒100-8220 東京都千代田区丸の内一丁目5番1号 株式会社 日立製作所内 Tokyo (JP).
- (81) 指定国 (国内): CA, JP, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
- 添付公開書類:
— 国際調査報告書
- 2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: ELLIPTIC CURVE GENERATING METHOD AND DEVICE, ELLIPTIC ENCRYPTION SYSTEM AND RECORDING MEDIUM

(54) 発明の名称: 楕円曲線生成方法 装置及び楕円暗号システム並びに記録媒体



- 101 ... ELLIPTIC CURVE PARAMETER GENERATING DEVICE
- 102 ... CONVERSION POSSIBILITY DECISION UNIT
- 103 ... DEFINITION OBJECT INFORMATION
- 104 ... STANDARD ELLIPTIC CURVE CANDIDATE GENERATING UNIT
- 106 ... COFACTOR DECISION UNIT
- 107 ... CURVE ORDER INFORMATION GATHERING UNIT
- 108 ... CURVE PARAMETER

(57) Abstract: A method and device for generating a safe standard elliptic curve that can be converted into a Montgomery elliptic curve, an elliptic encryption system and a recording medium, wherein a curve parameter generating device is constituted which gives a decision condition under which a curve order-related condition is separated from a decision condition whether or not a standard elliptic curve can be converted into a Montgomery elliptic curve and which incorporates a conversion possibility decision unit. For a method of generating a curve having a cofactor of 4, a condition under which a curve order can be divided by 8 is given.

[続葉有]



WO 01/18772 A1



(57) 要約:

本発明の目的は、モンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成方法、装置及び楕円暗号システム並びに記録媒体を提供することにある。

この目的を達成するために、標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かの判定条件から曲線位数に関する条件を切り離した判定条件を与え、変換可能判定部を組み込んだ曲線パラメタ生成装置を構成する。また、コファクタが4である曲線の生成方法に関しては、曲線位数が8で割れる条件を与える。

明 細 書

楕円曲線生成方法、装置及び楕円暗号システム並びに記録媒体

5

技術分野

本発明はコンピュータネットワークにおけるセキュリティ技術に係り、特に楕円暗号において用いる楕円曲線の生成方法、楕円曲線の装置及び楕円暗号システム並びにその方法を格納した記録媒体に関する。

10

背景技術

楕円暗号において用いる楕円曲線として、標準型楕円曲線 $y^2 = f(x)$ 、ただし $f(x) = x^3 + ax + b$ ($a, b \in F_p$)、 F_p は要素数が p 個の有限体で p は大きな素数、を用いることがある。 $y_0^2 = f(x_0)$ をみたす (x_0, y_0) の組 $(x_0, y_0 \in F_p)$ を曲線上の点といい、それら点全体に無限遠点を付け加えた集合に演算を入れることができ、その点の個数を曲線位数という。曲線位数を n として $n = cl$ と正整数 c と大きな素数 l と表した時、 c をコファクタといい、 c の値が小さい時にその楕円曲線を安全という。安全な標準型楕円曲線の生成方法として、ランダムに標準型楕円曲線を生成しその曲線位数により安全性を判定し、安全となるまで標準型楕円曲線の再生成を行う方法が ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), (1999) に記載されている。

20

また、モンゴメリ型楕円曲線 $BY^2 = X^3 + AX^2 + X$ ($A, B \in F_p$) を用いると標準型楕円曲線よりも高速に演算を実行できることが P. L. Montgomery, Speeding the Pollard and Elliptic Curve

25

Methods of Factorization, Math. Comp. 48 (1987) 243-264. に記載されている。標準型楕円曲線がモンゴメリ型楕円曲線に変換可能とは、標準型楕円曲線上の点とモンゴメリ型楕円曲線上の点とが1対1に対応し、それぞれにおける演算が一致することをいう。全ての標準型楕円曲線がモンゴメリ型楕円曲線に変換可能であるわけではない。伊豆哲也氏による「楕円曲線暗号演算の計算方法について」1999年暗号と情報セキュリティシンポジウム予稿集 vol. 1, (1999) 275-280. には標準型楕円曲線からモンゴメリ型楕円曲線への変換が可能なための条件が記載されている。さらにモンゴメリ型楕円曲線の曲線位数が必ず4で割れることも上記資料に記載されている。

上記従来技術はモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の生成に関しては考慮されていなかった。そのためにモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成のためには、安全な標準型楕円曲線を生成した後に、それがモンゴメリ型楕円曲線に変換可能かどうかを判定し、変換不可能であれば安全な標準型楕円曲線を再生成し、変換可能となるまで繰り返すといった手順を踏まなければならなかった。一般的に、安全な標準型楕円曲線を生成する処理は、モンゴメリ型楕円曲線に変換可能かどうかを判定する処理より時間を要する。そのため上記性質を持った楕円曲線の生成には多大な時間を必要とし、ネットワークセキュリティを確保するための楕円暗号において、定期的

に使用している楕円曲線を上記性質を持った新しい楕円曲線に置き換えることは難しかった。ここで、公開鍵を知らなくても楕円曲線のみを知っていれば攻撃のための前計算を行なえる攻撃法 (Baby-Step-Giant-Step 法) に対しては、楕円曲線を定期的に新しいものに置き換える以外に安全性を保つ方法は存在しないと言われている。したがって、従来技術を用いた場合は、特定楕円曲線に対する攻撃を受け易い状態に

あった。

本発明の目的は演算の高速性及び安全性を向上させる楕円曲線生成方法、装置及び楕円暗号システム並びに記録媒体を提供することにある。

5 発明の開示

上記目的は、楕円曲線の生成方法であって、第1の楕円曲線（例えば、 $y^2 = x^3 + ax + b$ ）を生成するステップと、前記第1の楕円曲線が第2の楕円曲線（例えば、 $BY^2 = X^3 + AX^2 + X$ ）に変換可能であるかを判定するステップと、前記第2の楕円曲線に変換可能な第1の楕円曲線の安全性を判定するステップとを有することにより達成する。ここで第1の楕円曲線は、予め定められた素数位数の体上定義された第1の楕円曲線を用いても良い。また、前記第2の楕円曲線に変換可能であるかを判定するステップは、前記第1の楕円曲線 $y^2 = f(x) = x^3 + ax + b$ に対して、 $f(\alpha) = 0$ となる α が存在するかを判定するステップと、 $f(\alpha) = 0$ となる α に対して $f'(\alpha)$ が平方根を持つかを判定するステップとからなることにより達成する。また、前記第1の楕円曲線の安全性を判定するステップは、前記第1の楕円曲線の曲線位数に関する情報を抽出するステップと、前記曲線位数に関する情報からコファクタの判定を行うステップとを有することにより達成する。また、第1の楕円曲線 $y^2 = x^3 + ax + b$ と第2の楕円曲線 $y^2 = x^3 + ar^2x + br^3$ とを生成するステップと、前記第1の楕円曲線が第3の楕円曲線 $BY^2 = X^3 + AX^2 + X$ に変換可能であるかを判定するステップと、前記第1の楕円曲線が前記第3の楕円曲線に変換可能である場合、前記第1の楕円曲線及び前記第2の楕円曲線の安全性を判定するステップとを有することにより達成する。また、楕円暗号における素体上定義された楕円曲線の生成方法であって、ランダムな標準型楕円曲線 $y^2 = x^3$

+ $ax + b$ を生成するステップと、前記生成された標準型楕円曲線 $y^2 = x^3 + ax + b$ がモンゴメリ型楕円曲線 $BY^2 = X^3 + AX^2 + X$ に変換可能であるかを判定するステップと、前記楕円曲線の曲線位数の 8 による整除性を判定するステップと、前記楕円曲線の曲線位数に関する情報を収集するステップと、前記曲線位数の情報からコファクタの値を判定するステップとからなり、モンゴメリ型楕円曲線に変換可能であり且つコファクタが 4 である標準型楕円曲線を生成することにより達成する。

また、楕円曲線生成装置であって、第 1 の楕円曲線 $y^2 = x^3 + ax + b$ を生成する楕円曲線候補生成部と、前記第 1 の楕円曲線が第 2 の楕円曲線 $BY^2 = X^3 + AX^2 + X$ に変換可能であるかを判定する変換可能判定部と、前記第 2 の楕円曲線に変換可能な第 1 の楕円曲線の安全性を判定する安全性判定部とを備えたことにより達成する。ここで、前記変換可能判定部は、前記第 1 の楕円曲線に対して、 $f(\alpha) = 0$ となる α が存在するかを判定する根存在判定部と、 $f(\alpha) = 0$ となる α に対して $f'(\alpha)$ が平方根を持つかを判定する平方根判定部とからなることにより達成する。また、前記変換可能判定部は、前記第 1 の楕円曲線に対して、 $f(\alpha) = 0$ となる α が存在するかを判定する根存在判定部と、 $f(\alpha) = 0$ となる α に対して $f'(\alpha)$ が平方剰余であるかを判定する平方剰余判定部とからなることにより達成する。また、第 1 の計算機と第 2 の計算機との間で暗号化通信を行う暗号システムで使用される楕円曲線生成装置であって、前記計算機から楕円曲線の生成要請を受け、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を生成することにより達成する。

また、楕円暗号を利用して暗号化通信を行う暗号システムであって、暗号化通信を受信する第 1 の計算機と、暗号化通信を送信する第 2 の計算機と、前記第 1 の計算機から楕円曲線の生成要請を受けて、モンゴメ

り型楕円曲線に変換可能な標準型楕円曲線を生成する楕円曲線生成装置とを備えたことにより達成する。また、暗号化通信に使用している楕円曲線に置換の必要性があるか否かを管理する曲線置換管理装置を更に備え、前記楕円曲線に置換の必要性が生じた場合は、前記楕円曲線生成装置が新たに生成した楕円曲線に置換して暗号化通信を行うことにより達成する。尚、上記目的を達成するためには、上述した方法、装置及びシステムで実現している機能を実現するプログラムを格納した記録媒体であっても良い。

10 図面の簡単な説明

第1図は、本発明の第1実施例において楕円暗号システムにおける曲線パラメタ生成サーバ内での楕円曲線の生成方法及び装置における処理の流れを示す図である。第2図は、本発明の第1実施例を示す楕円曲線の生成方法及び装置におけるモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成方法を示すフローチャートである。第3図は、本発明の楕円曲線の生成方法及び装置内の変換可能判定部における標準型楕円曲線からモンゴメリ型楕円曲線に変換可能かの判定方法を示すフローチャートである。第4図は、本発明の第1、2実施例の応用例を示す楕円曲線の生成方法及び装置におけるモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成方法を示すフローチャートである。第5図は、本発明の第2実施例の楕円暗号システムにおける曲線パラメタ生成サーバ内での楕円曲線の生成方法及び装置における処理の流れを示す図である。第6図は、本発明の第2実施例を示す楕円曲線の生成方法及び装置におけるモンゴメリ型楕円曲線に変換可能であり且つコファクタが4である標準型楕円曲線の生成方法を示すフローチャートである。第7図は、本発明の第2実施例における楕円曲線

パラメタ生成装置内でのモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数に対する8による整除性の判定方法を示すフローチャートである。特に、定義体素数が4を法として1の場合の判定方法を示している。第8図は、本発明の第2実施例における楕円曲線パラメタ生成装置内でのモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数に対する8による整除性の判定方法を示すフローチャートである。特に定義体素数が4を法として3の場合の判定方法を示している。第9図は、本発明の第2実施例で8による整除性の判定のための条件を列挙している表である。第10図は、本発明の第3実施例の楕円暗号システムにおける曲線パラメタ生成サーバ内での楕円曲線の生成方法及び装置における処理の流れを示す図である。第11図は、本発明の第3実施例を示す楕円曲線の生成方法及び装置におけるモンゴメリ型楕円曲線に変換可能であり且つコファクタが4である標準型楕円曲線の生成方法を示すフローチャートである。第12図は、本発明の第3実施例における標準型楕円曲線に対する適当性判定方法を示すフローチャートである。特に、定義体素数が4を法として1の場合の判定方法を示している。第13図は、本発明の第3実施例における標準型楕円曲線に対する適当性判定方法を示すフローチャートである。特に定義体素数が4を法として3の場合の判定方法を示している。第14図は、本発明の楕円暗号システムの一例の構成図である。第15図は、本発明の第4実施例における楕円暗号システムでの曲線生成方法に関するフローチャートである。第16図は、本発明の第5実施例における楕円暗号システムの構成図である。第17図は、本発明の第5実施例における楕円暗号システムでの曲線生成方法に関するフローチャートである。第18図は、本発明の第6実施例における楕円暗号システムの構成図である。第19図は、本発明の第6実施例における楕円暗号システムでの曲線生成方法に関するフロー

チャートである。第 20 図は、本発明の第 7 実施例における楕円暗号システム
の構成図である。第 21 図は、本発明の第 7 実施例における楕円
暗号システムでの曲線生成方法に関するフローチャートである。第 22
図は、楕円曲線パラメタ生成装置内での標準型楕円曲線からモンゴメリ
5 型楕円曲線への変換判定方法及び装置における処理の流れを示す図であ
る。第 23 図は、本発明の楕円暗号システムにおける曲線パラメタ変換
装置での標準型楕円曲線からモンゴメリ型楕円曲線への変換における処
理の流れを示す図である。第 24 図は、曲線パラメタ変換方法を示すフ
ローチャートである。第 25 図は、本発明の楕円曲線パラメタ生成装置
10 内での標準型楕円曲線からモンゴメリ型楕円曲線への変換可能判定方法
及び装置における処理の流れを示す図である。第 26 図は、標準型楕円
曲線からモンゴメリ型楕円曲線への変換可能判定方法を示すフロー
チャートである。第 27 図は、本発明の実施例におけるデータ構造であ
る。第 28 図は、曲線置換管理装置の一実施例を示す図である。第 29
15 図は、曲線置換管理装置を公開鍵サーバに組み込んだ楕円暗号システム
での曲線パラメタ置換における処理の流れを示すシーケンス図である。

発明を実施するための最良の形態

以下、本発明の一実施例を図面により説明する。図 14 は本発明が
20 適用される楕円暗号システムの構成図の一例である。

まず、楕円曲線暗号システムを構成する曲線パラメタ生成サーバ内
の楕円曲線パラメタ生成装置について図 1、図 2 を用いて説明する。図
1 は楕円暗号システムにおける曲線パラメタ生成サーバ内でのモンゴメ
リ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成方法の
25 第 1 実施例を示す図である。図 2 は第 1 実施例の楕円曲線パラメタ生成
装置 101 における標準型楕円曲線の曲線パラメタの生成方法を示すフ

ローチャートである。

楕円曲線パラメタ生成装置 101 では、定義体情報 103 を入力し、以下の手順により曲線パラメタ 108 を出力する。ここで定義体情報 103 は図 27 における、定義体のビット長を含んだ定義体情報 2701 5 もしくは定義体素数を含んだ定義体情報 2704 で与えられている。楕円曲線候補生成部 104 において、定義体情報 103 よりランダムな標準型楕円曲線を生成する（ステップ 201）。ランダムな標準型楕円曲線の生成方法については ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), (1999) に記述されている。変換可能判定部 102 において楕円曲線候補生成部 104 で生成された標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かの判定を行なう（ステップ 202）。変換不可能であれば楕円曲線候補生成部 104 で標準型楕円曲線の再生成を行ない、変換可能となるまで繰り返す。曲線位数情報収集部 107 では変換可能判定部 102 によりモンゴメリ型楕円曲線に変換可能と判断された標準型楕円曲線の曲線位数に関する情報を収集する（ステップ 204）。与えられた楕円曲線の曲線位数に関する情報を収集することにより曲線位数を決定する曲線位数決定方法については R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Math. Comp. 44 (1985), 483-494 に記載されている。コファクタ判定部 106 では曲線位数情報収集部 107 により取得した曲線位数の情報からコファクタが安全性の条件より与えられる値より小さいかどうかを判定し（ステップ 205）、コファクタの値が大きければ、楕円曲線候補生成部 104 により標準型楕円曲線の再生成を行ない、上記手順に従ってモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数に関する情報から、再

度コファクタ判定部 106 によりコファクタの値が小さいかどうかの判定を行ない、コファクタの値が小さいと判定されるまで以上の手順を繰り返す。コファクタの値が小さければ、上記手順により生成されたモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線を曲線パラメタとして出力を行なう（ステップ 206）。

変換可能判定部 102 では以下の手順により標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かを判定する。ここで、変換可能判定の一実施例を図 3 のフローチャートを用いて説明する。解の存在判定において標準型楕円曲線 $y^2 = f(x) = x^3 + ax + b$ に対して $f(\alpha) = 0$ となる F_p の元 α が存在するかを調べる（ステップ 301）。そのような元 α が存在しなければ変換不可能と出力し終了する（ステップ 304）。上記 α が存在すれば、平方剰余判定により、 $f(\alpha) = 0$ となる α に対して、 $f'(\alpha)$ が F_p において平方剰余となる α が存在するかを判定する（ステップ 302）。そのような α が存在すれば変換可能と出力し終了する（ステップ 303）。そのような α が存在しなければ変換不可能と出力して終了する（ステップ 304）。ここで平方剰余とは素数 p を法として平方根が存在する時をいい、存在しない場合は平方非剰余という。

以上の手順により変換可能の判定ができるということの根拠は以下の通りである。モンゴメリ型楕円曲線には $(0,0)$ という 2 倍すると無限遠点となる点があり、標準型楕円曲線には一般的にはそのような点があるとは限らないので、変換可能となるためには、標準型楕円曲線上の点で、2 倍すると無限遠点になる点の存在が必要である。一般に m 倍して初めて無限遠点となる点のことを位数 m の点という。 $f(\alpha) = 0$ となる α に対して、 $(\alpha, 0)$ は位数 2 の点である。変換可能とすれば、標準型楕円曲線上の位数 2 の点で、変換後に $(0,0)$ へ移る点が必要であり、 $(\alpha, 0)$ がそのような点とした場合に、標準型楕円曲線の点からモンゴメリ型楕円

10

曲線の点への変換は、ある $s, t \in F_p$ に対して $X = s(x - \alpha), Y = ty$ ($s \neq 0, t \neq 0$) と表されなければならない。 (X, Y) はモンゴメリ型楕円曲線上の点であるので $BY^2 = X^3 + AX^2 + X$ をみたし、 X, Y にそれぞれ $s(x - \alpha), ty$ を代入すると、 $Bt^2y^2 = s^3(x - \alpha)^3 + As^2(x - \alpha)^2 + s(x - \alpha)$ となる。

5 (x, y) は標準型楕円曲線上の点であるので、この式に $y^2 = f(x)$ を代入すると、 $Bt^2f(x) = s^3(x - \alpha)^3 + As^2(x - \alpha)^2 + s(x - \alpha)$ となる。 x^3 の項を比較することにより、 $Bt^2 = s^3$ を得る。これを上の式に代入すると、 $s \neq 0$ であるから、 $s^2f(x) = s^2(x - \alpha)^3 + As(x - \alpha)^2 + (x - \alpha)$ となる。この式を x で微分し、 x に α を代入すると、 $s^2f'(\alpha) = 1$ を得る。 s は F_p の元であるから、
10 $f'(\alpha)$ は平方剰余でなければならない。またその時、 $A = 3\alpha s, B = s^3/t^2$ である。逆に $f'(\alpha)$ が平方剰余であれば、 $s = t = f'(\alpha)^{-1/2}, A = 3\alpha s, B = s$ とおけばモンゴメリ型楕円曲線 $BY^2 = X^3 + AX^2 + X$ に変換可能である。

以上により、変換可能であるためには、モンゴメリ型楕円曲線及び標準型楕円曲線上のそれぞれ位数 2 の点がお互いに移りあうことが必要
15 であることを基にして、上記手順により変換可能の判定を行なえることが示された。

またモンゴメリ型楕円曲線の曲線位数は 4 で割れることが次のようにして分かる。モンゴメリ型楕円曲線上の点 $(0, 0)$ は位数 2 の点である。 $X^2 + AX + 1$ の判別式 $A^2 - 4$ が平方剰余であれば、 $X^2 + AX + 1$ は F_p において根を持ち、したがって $(0, 0)$ 以外に位数 2 の点が 2 つ存在するので曲
20 線位数は 4 で割れる。 $A^2 - 4$ が平方非剰余であれば、 $A + 2$ 及び $A - 2$ のうち一方のみが平方剰余であり他方は平方非剰余である。そのため $(A + 2)/B$ 及び $(A - 2)/B$ の一方が平方剰余となる。 $(A + 2)/B$ が平方剰余の場合はその平方根を γ として $(1, \pm\gamma)$ が、 $(A - 2)/B$ が平方剰余の時はその平方根を γ' として $(-1, \pm\gamma')$ がそれぞれ位数 4 の点となり、曲線位数は 4
25 で割れる。したがっていずれの場合においても曲線位数は 4 で割れる。

ここで、楕円曲線における演算速度は定義体の大きさに依存し、大きくなると遅くなる。楕円曲線の安全性は曲線位数に含まれる最大の素数の大きさに依存し、大きければ安全である。定義体の大きさを固定した時に、安全性を高くするためにはコファクタを小さくしなければならない。モンゴメリ型楕円曲線の曲線位数は4で割れるのでコファクタは4以上となり、定義体の大きさを固定してもっとも安全性を高めるにはコファクタは4にする必要がある。

尚、曲線位数を変換可能の判定条件に使わなければ、他の変換判定条件を用いることもできる。文献「楕円曲線暗号演算の計算方法について」1999年暗号と情報セキュリティシンポジウム予稿集 vol. 1, (1999) 275-280. の278ページにはそのような方法が記載されている。

次に、図14の楕円暗号システムにおける曲線パラメタ生成サーバ1401内でのモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成方法の第1実施例の応用例を図1、図4を用いて説明する。図4は、楕円曲線パラメタ生成装置101における標準型楕円曲線の曲線パラメタの生成方法を示すフローチャートである。

楕円曲線パラメタ生成装置101では、定義体情報103を入力し、以下の手順により曲線パラメタ108を出力する。ここで定義体情報103は図27における、定義体のビット長を含んだ定義体情報2701もしくは定義体素数を含んだ定義体情報2704で与えられている。楕円曲線候補生成部104において、定義体情報103よりランダムな標準型楕円曲線を生成する（ステップ401）。標準型楕円曲線 $y^2 = f(x) = x^3 + ax + b$ に対して、標準型楕円曲線 $y^2 = f_r(x) = x^3 + ar^2x + br^3$ を標準型楕円曲線 $y^2 = x^3 + ax + b$ のツイストという。ただし、 r は F_p において平方非剰余な元である。ツイストに対し

て標準型楕円曲線 $y^2 = x^3 + ax + b$ を明示的にいう場合にはオリジナルという。変換可能判定部 102 において楕円曲線候補生成部 104 で生成された標準型楕円曲線及びそのツイストの標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かの判定を行なうステップ (402)。オリジナルの標準型楕円曲線が変換可能であればツイストの標準型楕円曲線も変換可能である。共に変換不可能であれば楕円曲線候補生成部 104 で標準型楕円曲線の再生成を行ない、変換可能となるまで繰り返す。曲線位数情報収集部 107 では変換可能判定部 102 によりモンゴメリ型楕円曲線に変換可能と判断されたオリジナル及びツイストの標準型楕円曲線の曲線位数に関する情報を収集する (ステップ 403)。コファクタ判定部 106 では曲線位数情報収集部 107 により取得したオリジナル及びツイストの曲線位数の情報からそれぞれのコファクタが安全性の条件から与えられる値より小さいかどうかを判定し (ステップ 404)、共にコファクタが大きければ、楕円曲線候補生成部 104 により標準型楕円曲線の再生成を行ない、上記手順に従ってモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数に関する情報から、再度コファクタ判定部 106 によりそれぞれのコファクタが小さいかどうかの判定を行ない、いずれかのコファクタが小さいと判定されるまで以上の手順を繰り返す。いずれかのコファクタが小さければ、上記手順により生成されたモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線を曲線パラメタとして出力を行なう (ステップ 405)。以上の応用例では、オリジナル及びツイストの標準型楕円曲線のモンゴメリ型楕円曲線への変換可能性の判定を一度に行うため、安定性判定を行う標準型楕円曲線の候補を増やせることとなり、更に曲線生成が高速化される。

オリジナルの標準型楕円曲線がモンゴメリ型楕円曲線に変換可能である時、そのツイストの標準型楕円曲線もモンゴメリ型楕円曲線に変換

可能であることの根拠は以下の通りである。オリジナルの標準型楕円曲線がモンゴメリ型楕円曲線に変換可能であるので、 $f(\alpha)=0$ 且つ $f'(\alpha)$ が平方剰余である α が存在する。その時 $f_r(r\alpha)=0$ であり、 $f'_r(r\alpha)=r^2f'(\alpha)$ であるので $f'_r(r\alpha)$ は平方剰余である。従ってツイストの標準型楕円曲線もモンゴメリ型楕円曲線に変換可能である。また、オリジナルの標準型楕円曲線はツイストの標準型楕円曲線のツイストであるため、ツイストの標準型楕円曲線がモンゴメリ型楕円曲線に変換可能であればオリジナルの楕円曲線もモンゴメリ型楕円曲線に変換可能である。オリジナルの標準型楕円曲線 $y^2 = x^3 + ax + b$ がモンゴメリ型楕円曲線 $BY^2 = X^3 + AX^2 + X$ に変換される時、ツイストの標準型楕円曲線 $y^2 = x^3 + ar^2x + br^3$ はモンゴメリ型楕円曲線 $(B/r)Y^2 = X^3 + AX^2 + X$ に変換される。

図5は楕円暗号システムにおける曲線パラメタ生成サーバ内でのモンゴメリ型楕円曲線に変換可能であり且つその曲線位数が $4 \times$ 素数である、すなわちコファクタが4である標準型楕円曲線の生成方法の第2実施例を示す図である。図6は、第2実施例における楕円曲線パラメタ生成装置501におけるモンゴメリ型楕円曲線に変換可能且つコファクタが4である標準型楕円曲線の曲線パラメタの生成方法を示すフローチャートである。上述したとおり、モンゴメリ型楕円曲線に変換可能であるとすると、曲線位数が4の倍数になる。そのうち、安全性を高くするためには、曲線位数が $4 \times$ 素数が望ましい。

楕円曲線パラメタ生成装置501では定義体情報503を入力し、以下の手順により曲線パラメタ508を出力する。ここで定義体情報503は図27における、定義体のビット長を含んだ定義体情報2701もしくは定義体素数を含んだ定義体情報2704で与えられている。標準型楕円曲線候補生成部504において、定義体情報503よりランダ

ムな標準型楕円曲線を生成する（ステップ601）。変換可能判定部502において楕円曲線候補生成部で生成された標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かの判定を行なう（ステップ602）。変換不可能であれば標準型楕円曲線候補生成部504で標準型楕円曲線の再生成を行ない、変換可能となるまで繰り返す。8による整除性判定部505では変換可能判定部502によりモンゴメリ型楕円曲線に変換可能と判断された標準型楕円曲線の曲線位数が8で割れるかどうかを判定する（ステップ603）。上記楕円曲線の曲線位数が8で割れれば、楕円曲線候補生成部504により標準型楕円曲線の再生成を行ない、上記手順に従ってモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数が8で割れるかの判定を行ない、曲線位数が8で割れないと判定されるまで以上の手順を繰り返す。曲線位数が8で割れなければ、曲線位数情報収集部507により、モンゴメリ型楕円曲線に変換可能であり且つその曲線位数が8で割れない標準型楕円曲線の、曲線位数に関する情報を収集する（ステップ604）。コファクタ判定部506では曲線位数情報収集部507により取得した曲線位数の情報からコファクタが4であるかを判定し（ステップ605）、コファクタが4を越えると判定されれば、楕円曲線候補生成部504により標準型楕円曲線の再生成を行ない、上記手順に従ってモンゴメリ型楕円曲線に変換可能であり且つその曲線位数が8で割れない標準型楕円曲線の曲線位数に関する情報から、再度コファクタ判定部506によりコファクタが4であるかの判定を行ない、コファクタが4と判断されるまで以上の手順を繰り返す。コファクタが4であれば、上記手順により生成されたモンゴメリ型楕円曲線に変換可能であり且つそのコファクタが4である標準型楕円曲線を曲線パラメタとして出力を行なう（ステップ606）。

8による整除性判定部505は、以下の手順によりモンゴメリ型楕

円曲線に変換可能な標準型楕円曲線の曲線位数が8で割れるかどうかを判定する。図7及び図8は第2実施例における8による整除性判定方法を示すフローチャートである。

5 ステップ701により定義体素数が4を法として1であるか3であるかに応じて以下の処理を振り分ける。定義体素数の4を法とした値が1であればステップ702へ、3であればステップ801へ行く。ステップ702において、 $f(x)=0$ の F_p における根の数により処理を振り分ける。根の数が1個であればステップ704へ、3個であればステップ703へ行く。ステップ703において、 $(A+2)/B$ が F_p において平方剰余であるかを判定する。平方剰余であれば曲線位数は8で割れる
10 (ステップ705)。平方非剰余であれば曲線位数は8で割れない(ステップ706)。ステップ704において $f'(\alpha)^{1/2}$ が F_p において平方剰余であるかを判定する。平方非剰余であれば曲線位数は8で割れない(ステップ706)。平方剰余であれば曲線位数は8で割れる(ステップ705)。以上により、定義体素数の4を法とする値が1の時に対して曲線位数が8で割れるかを判定できる。定義体素数の4を法とする値が3の場合は、ステップ801において $f(x)=0$ の F_p における根の数により処理を振り分ける。根の数が1個であればステップ802へ、3個であれば曲線位数は8で割れる(ステップ705)。ステップ802において、 $A+2$ が F_p において平方剰余であるかを判定する。平方非剰余であれば曲線位数は8で割れない(ステップ706)。平方剰余であれば曲線位数は8で割れる(ステップ705)。以上により、定義体素数の4を法とする値が3の時に対して曲線位数が8で割れるかを判定できる。

25 以上の手順により、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線の曲線位数に対する8による整除性の判定ができるということの根

5 抛は以下の通りである。 $BY^2 = X^3 + AX^2 + X$ を標準型楕円曲線から変換
 されたモンゴメリ型楕円曲線とする。まず $f(x)=0$ の F_p における根の数
 を1個とする。この時標準型楕円曲線上の点で位数が2であるものは
 $(\alpha, 0)$ ただ一つである。モンゴメリ型楕円曲線上の位数2の点の x 座標は
 10 $X^3 + AX^2 + X = 0$ の F_p 上での根であり、モンゴメリ型楕円曲線上の点
 $(0, 0)$ は標準型楕円曲線上の点 $(\alpha, 0)$ と対応するので、 $X^2 + AX + 1 = 0$ は F_p
 において根を持たない。従ってその判別式 $A^2 - 4$ は F_p において平方非剰
 余である。 $(A+2)/B$ 乃至 $(A-2)/B$ が平方剰余であれば、その平方根の
 1つをそれぞれ γ, γ' とすれば、 $(1, \pm\gamma)$ もしくは $(-1, \pm\gamma')$ が位数4の点と
 15 なる。 $A^2 - 4$ は平方非剰余であるので $(A+2)/B$ 及び $(A-2)/B$ のいずれ
 か一方は平方剰余でなければならない。従ってこの場合に必ず位数4の
 点が存在する。

モンゴメリ型楕円曲線上のある点 (u, v) がこの曲線上の他の点 (w, z) の
 2倍点となると仮定する。点 (w, z) における接線の式は
 15 $Y = ((3w^2 + 2Aw + 1)/2Bz)(X - w) + z$ である。接線は $(u, -v)$ で曲線と交わる
 ので (X, Y) に $(u, -v)$ を代入し、両辺に $2Bz$ を掛けて2乗すると
 $4Bv^2 Bz^2 = ((3w^2 + 2Aw + 1)(u - w) + 2Bz^2)^2$ となる。 (w, z) 及び $(u, -v)$ は曲線
 上の点であるので $Bz^2 = w^3 + Aw^2 + w$ 及び $Bv^2 = u^3 + Au^2 + u$ をみたとす。こ
 れを上式に代入すると $4(u^3 + Au^2 + u)(w^3 + Aw^2 + w) = ((3w^2 + 2Aw + 1)(u - w) + 2(w^3 + 2Aw^2 + w))^2$
 20 となる。点 (w, z) で曲線と接線は接していて、また w と u は異なるので、
 $(u - w)^2$ で割ることができ $(3w^2 + 2Aw + 1)^2 - 4(w^3 + Aw^2 + w)(u + A + 2w) = 0$
 となる。 w の式とみて整理すると $w^4 - 4uw^3 - (4Au + 2)w^2 - 4uw + 1 = 0$ とな
 り、 $w \neq 0$ なので、 w^2 で割って $w + 1/w$ の式とみて整理し直すと、
 $(w + 1/w)^2 - 4u(w + 1/w) - 4(Au + 1) = 0$ となる。 $w \in F_p$ とすると $1/w \in F_p$ であ
 25 り、 $w + 1/w \in F_p$ となる。上の式が $w + 1/w$ の方程式として F_p 上で根を持
 つためには、その判別式 $4(u^2 + Au + 1)$ が平方剰余でなければならない。

ε を $u^2 + Au + 1$ の平方根の一つとすると $w + 1/w = 2(u \pm \varepsilon)$ であり、この式
 が w の方程式として F_p 上で根を持つためには、判別式 $(u \pm \varepsilon)^2 - 1$ が平方
 剰余でなければならない。 $((u + \varepsilon)^2 - 1)((u - \varepsilon)^2 - 1) = u^2(A^2 - 4)$ であり、
 $A^2 - 4$ は平方非剰余であるので、 $(u + \varepsilon)^2 - 1$ 及び $(u - \varepsilon)^2 - 1$ のいずれか一
 5 方のみが平方剰余となる。その時 $w = (u \pm \varepsilon) \pm \sqrt{(u \pm \varepsilon)^2 - 1}$ であり、簡単
 のため $\delta = u \pm \varepsilon$ とおくと、 $w^2 + Aw + 1 = (2\delta + A)(\delta \pm \sqrt{\delta^2 - 1})$ なので
 $Bz^2 = (2\delta + A)(\delta \pm \sqrt{\delta^2 - 1})^2$ となり、 $z \in F_p$ であるためには $(2\delta + A)/B$ が平
 方剰余でなければならない。また、この場合も同様に
 $(2(u + \varepsilon) + A)(2(u - \varepsilon) + A) = A^2 - 4$ であるから、 $(2(u + \varepsilon) + A)/B$ もしくは
 10 $(2(u - \varepsilon) + A)/B$ のいずれか一方のみが平方剰余となる。上記平方剰余に
 関する2つの二者択一条件において、共に同じ符号をとれば、 $w, z \in F_p$
 となる。 $(u \pm \varepsilon)^2 - 1 = u(2(u \pm \varepsilon) + A)$ と変形すると、
 $((u \pm \varepsilon)^2 - 1)((2(u \pm \varepsilon) + A)/B) = (u/B)(2(u \pm \varepsilon) + A)^2$ となる。したがって、
 u/B が平方剰余であれば、上記平方剰余に関する2つの二者択一条件に
 15 いて共に同じ符号をとることができ、2倍すると点 (u, v) となる点
 (w, z) が存在する。以上をまとめると $u^2 + Au + 1, u/B$ が共に平方剰余であ
 れば、2倍すると点 (u, v) となる点 (w, z) が存在する、ということが示さ
 れた。

位数4の点の x 座標は ± 1 であり、したがって位数8の点の存在に関
 20 しては $A \pm 2, B, -1$ の平方剰余性により表すことができる。

-1 が平方剰余であるのは定義体素数が4を法として1の時であり、
 -1 が平方非剰余であるのは定義体素数が4を法として3の時である。
 $f(x) = 0$ の根の数が1個であるか3個であるかに応じて、 $A^2 - 4$ が平方
 非剰余であるか平方剰余であるかが決まる。オリジナル及びツイストの
 25 曲線位数を加えると $2(p+1)$ であるので、 $f(x) = 0$ の根の数が3個の場合
 において、定義体素数が4を法として1の時は、オリジナルの曲線位数

が8で割れればツイストの曲線位数は8で割れず、オリジナルの曲線位数が8で割れなければツイストの曲線位数は8で割れる。また、定義体素数が4を法として3の時は、オリジナルの曲線位数が8で割れればツイストの曲線位数も8で割れ、オリジナルの曲線位数が8で割れなければツイストの曲線位数も8で割れない。以上をまとめると図9の通りである。図9により、図7及び図8のフローチャートの手順で判定を行なえば、曲線位数の8による整除性を判定できる。

上記8による整除性判定方法において、ステップ802の $A+2$ の平方剰余判定は $A-2$ の平方剰余判定を用いても行なうことができる。
 $f(x)=0$ の根の数が1個の場合は A^2-4 は平方非剰余なので、 $A+2$ が平方剰余であれば $A-2$ は平方非剰余であり、 $A+2$ が平方非剰余であれば $A-2$ は平方剰余であるので、 $A-2$ の平方剰余判定により判定可能である。ステップ703の $A+2$ の平方剰余判定においても、 $f(x)=0$ の根の数が3個の場合は A^2-4 は平方剰余なので、 $(A+2)/B$ が平方剰余であれば $(A-2)/B$ も平方剰余であり、 $(A+2)/B$ が平方非剰余であれば $(A-2)/B$ も平方非剰余であるので、 $(A-2)/B$ の平方剰余判定により判定可能である。ステップ704の $f'(\alpha)^{1/2}$ の平方剰余判定においても、 $f'(\alpha)^{1/2}$ と B の平方剰余性は一致するので、 B の平方剰余判定により判定可能である。

尚、第2実施例では、コファクタが4の場合を最適な実施例として、8による整除性判定方法を用いたが、本発明はこれに限定されるわけではなく、曲線位数=コファクタ×素数の関係から導き出される他の整数であっても良い。

また、第2実施例においても、その応用例として図4を用いて説明した第1実施例の応用例と同様の方法が適用できる。

次に標準型楕円曲線の生成方法の第3実施例を説明する。

図10は楕円暗号システムにおける曲線パラメタ生成サーバ内での

モンゴメリ型楕円曲線に変換可能であり且つその曲線位数が $4 \times$ 素数である、すなわちコファクタが 4 である標準型楕円曲線の生成方法の第 3 実施例を示す図である。図 11 は、第 3 実施例における楕円曲線パラメタ生成装置 1001 におけるモンゴメリ型楕円曲線に変換可能且つコファクタが 4 である標準型楕円曲線の曲線パラメタの生成方法を示すフローチャートである。

楕円曲線パラメタ生成装置 1001 では定義体情報 1003 を入力し、以下の手順により曲線パラメタ 1008 を出力する。ここで定義体情報 1003 は図 27 における、定義体のビット長を含んだ定義体情報 2701 もしくは定義体素数を含んだ定義体情報 2704 で与えられている。楕円曲線候補生成部 1004 において、定義体情報 1003 よりランダムな標準型楕円曲線を生成する（ステップ 1101）。適当性判定部 1002 において楕円曲線候補生成部で生成された標準型楕円曲線及びそのツイストの標準型楕円曲線がモンゴメリ型楕円曲線に変換可能となり且つそれぞれの曲線位数が 8 で割れるかの判定を行なう（ステップ 1102）。変換不可能であったり、変換可能であってもオリジナル及びツイストの標準型楕円曲線の曲線位数が共に 8 で割れれば標準型楕円曲線候補生成部 1004 で標準型楕円曲線の再生成を行ない、モンゴメリ型楕円曲線に変換可能であり且つオリジナル及びツイストの標準型楕円曲線の曲線位数のいずれか一方が 8 で割れないと判断されるまで繰り返す。モンゴメリ型楕円曲線に変換可能であり且つオリジナル及びツイストの標準型楕円曲線のいずれか一方の曲線位数が 8 で割れなければ、曲線位数情報収集部 1007 により、モンゴメリ型楕円曲線に変換可能であり且つその曲線位数もしくはツイストの曲線位数が 8 で割れない標準型楕円曲線の、曲線位数に関する情報を収集する（ステップ 1103）。コファクタ判定部 1006 では曲線位数情報収集部 1007 によ

り取得した曲線位数の情報からコファクタが4であるかを判定し（ステップ1104）、コファクタが4を越えれば、楕円曲線候補生成部1004により標準型楕円曲線の再生成を行ない、上記手順に従ってモンゴメリ型楕円曲線に変換可能であり且つその曲線位数が8で割れない標準型楕円曲線の曲線位数に関する情報から、再度コファクタ判定部1006によりコファクタが4であるかの判定を行ない、コファクタが4と判断されるまで以上の手順を繰り返す。コファクタが4であれば、上記手順により生成されたモンゴメリ型楕円曲線に変換可能であり且つそのコファクタが4である標準型楕円曲線を曲線パラメタとして出力を行なう（ステップ1105）。

標準型楕円曲線に対する適当性判定部1002は、与えられた標準型楕円曲線及びそのツイストの標準型楕円曲線が、モンゴメリ型楕円曲線に変換可能であり且つそれぞれの曲線位数が8で割れるかどうかを判定する。図12及び図13は第3実施例における標準型楕円曲線に対する適当性判定方法を示すフローチャートである。

ステップ1201により定義体素数が4を法として1であるか3であるかに応じて以下の処理を振り分ける。定義体素数の4を法とした値が1であればステップ1202へ、3であればステップ1301へ行く。ステップ1202において、 $f(x)=0$ の F_p における根の数により処理を振り分ける。根の数が1個であればステップ1204へ、3個であればステップ1203へ行く。 $f(x)=0$ が F_p において根を持たなければ、オリジナル及びツイストの標準型楕円曲線は共にモンゴメリ型楕円曲線に変換不可能であり不適當（1209）である。ステップ1203において、 $f(\alpha)=0$ となる α のうち $f'(\alpha)$ が F_p において平方剰余であるものを選択する。この α に関して標準型楕円曲線はモンゴメリ型楕円曲線に変換可能である。ステップ1205において、 $(A+2)/B$ が F_p において平

方剰余であるかを判定する。平方剰余であればオリジナルの標準型楕円曲線の曲線位数は8で割れ、ツイストの標準型楕円曲線の曲線位数は8で割れないので、ツイストを選択する（ステップ1207）。平方非剰余であればツイストの標準型楕円曲線の曲線位数は8で割れ、オリジナルの標準型楕円曲線の曲線位数は8で割れないので、オリジナルを選択する（ステップ1208）。ステップ1204において、 $f'(\alpha)$ が F_p において平方剰余であるかを判定する。平方非剰余であれば、オリジナル及びツイストの標準型楕円曲線は共にモンゴメリ型楕円曲線に変換不可能であり不適当（1209）である。平方剰余であればステップ1206へ行く。この場合、標準型楕円曲線はモンゴメリ型楕円曲線に変換可能である。ステップ1206において $f'(\alpha)^{1/2}$ が F_p において平方剰余であるかを判定する。平方非剰余であればツイストの標準型楕円曲線の曲線位数は8で割れ、オリジナルの標準型楕円曲線の曲線位数は8で割れないので、オリジナルを選択する（ステップ1208）。平方剰余であればオリジナルの標準型楕円曲線の曲線位数は8で割れ、ツイストの標準型楕円曲線の曲線位数は8で割れないので、ツイストを選択する（ステップ1207）。以上により、定義体素数の4を法とする値が1の時に對して、与えられたオリジナル及びツイストの標準型楕円曲線に對して、モンゴメリ型楕円曲線に変換可能であり且つ曲線位数が8で割れない標準型楕円曲線を選択する、あるいは不適当であるとして棄却するための判定を実行できる。定義体素数の4を法とする値が3の場合は、ステップ1301において $f(x)=0$ の F_p における根の数により処理を振り分ける。根の数が1個であればステップ1302へ、3個もしくは $f(x)=0$ が F_p において根を持たなければ、与えられたオリジナル及びツイストの標準型楕円曲線は共に変換不可能であったり変換可能であってもオリジナル及びツイストの曲線位数が共に8で割れるので不適当であ

る（ステップ 1 2 0 9）。ステップ 1 3 0 2 において、 $f'(\alpha)$ が F_p において平方剰余であるかを判定する。平方非剰余であれば、オリジナル及びツイストの標準型楕円曲線は共に変換不可能であり不適當である（1 2 0 9）。平方剰余であればステップ 1 3 0 3 へ行く。この場合与えられたオリジナル及びツイストの標準型楕円曲線は共にモンゴメリ型楕円曲線に変換可能である。ステップ 1 3 0 3 において、 $A+2$ が F_p において平方剰余であるかを判定する。平方非剰余であればオリジナル及びツイストの標準型楕円曲線の曲線位数は共に 8 で割れないので、オリジナル及びツイスト共に選択する（ステップ 1 3 0 5）。平方剰余であればオリジナル及びツイストの標準型楕円曲線の曲線位数は共に 8 で割れ、不適當である（ステップ 1 2 0 9）。以上により、定義体素数の 4 を法とする値が 3 の時に対して、与えられたオリジナル及びツイストの標準型楕円曲線に対して、モンゴメリ型楕円曲線に変換可能であり且つ曲線位数が 8 で割れない標準型楕円曲線を選択する、あるいは不適當であるとして棄却するための判定を実行できる。

以上の手順により、与えられたオリジナル及びツイストの標準型楕円曲線からモンゴメリ型楕円曲線に変換可能であり且つその曲線位数が 8 で割れない標準型楕円曲線を選択できる、あるいは不適當であるとして棄却できるということの根拠は以下の通りである。図 1 2 及び図 1 3 のフローチャートにおいて、前半は標準型楕円曲線がモンゴメリ型楕円曲線に変換可能であるかを判定しており、後半はモンゴメリ型楕円曲線に変換可能である標準型楕円曲線に対して、図 9 に基づき曲線位数が 8 で割れるかを判定している。オリジナルの標準型楕円曲線に対応するモンゴメリ型楕円曲線とツイストの標準型楕円曲線に対応するモンゴメリ型楕円曲線において、それぞれの Y^2 の係数の平方剰余性は正反対になっていることに注意すればよい。ステップ 1 2 0 3 において $f'(\alpha)$ が

平方剰余となる α が必ず選択できる事については、 Δ を $f(x)$ の判別式とすると $f(x)=0$ の根が3個の場合に Δ は平方剰余であり、他方 α, β, γ を $f(x)=0$ の根とすると $\Delta = -16f'(\alpha)f'(\beta)f'(\gamma)$ であるので、 $f'(\alpha), f'(\beta), f'(\gamma)$ のうち少なくとも1つは平方剰余である。

- 5 次に、図14を用いて、モンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムを第4実施例として説明する。

- 10 曲線パラメタ生成サーバ1401は第1実施例におけるモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を行なう楕円曲線パラメタ生成装置101を組み込んだサーバである。コンピュータA1402はモンゴメリ型楕円曲線を利用した楕円暗号により暗号化通信を行なうための秘密鍵公開鍵の組の生成を行なおうとしているコンピュータである。公開鍵サーバ1403は各コンピュータの公開鍵の登録を行ない、問い合わせがあれば問い合わせ対象のコンピュータの公開鍵を送信する。コンピュータB1404はコンピュータA1402へモンゴメリ型楕円曲線を利用して楕円暗号により暗号化通信を行なおうとしているコンピュータである。

- 20 第4実施例における楕円暗号システムでは以下の手順により楕円曲線パラメタ生成装置を利用して暗号化通信を行なう。図15はそのフローチャートである。コンピュータA1402は曲線パラメタ生成サーバ1401にモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を要請する（ステップ1501）。曲線パラメタ生成サーバ1401は上記曲線の生成要請に基づき、定義体情報103を楕円曲線パラメタ生成装置101に与えて曲線パラメタ108を生成する
- 25 （ステップ1502）。ここで定義体情報103は図27における、定義体のビット長を含んだ定義体情報2701もしくは定義体素数を含ん

だ定義体情報 2 7 0 4 で与えられている。新規曲線パラメタとして、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式及び曲線位数、標準型楕円曲線を変換したモンゴメリ型楕円曲線の定義式、及び標準型楕円曲線上の位数 2 の点でモンゴメリ型楕円曲線上の点 (0,0) に対応する点の x 座標をコンピュータ A 1 4 0 2 に渡す（ステップ 1 5 0 3）。コンピュータ A 1 4 0 2 は与えられた新規曲線パラメタから秘密鍵公開鍵の組を作成する（ステップ 1 5 0 4）。コンピュータ A 1 4 0 2 は公開鍵サーバ 1 4 0 3 に上記作成した公開鍵を登録する（ステップ 1 5 0 5）。コンピュータ B 1 4 0 4 は公開鍵サーバ 1 4 0 3 にコンピュータ A 1 4 0 2 の公開鍵の問い合わせを行なう（ステップ 1 5 0 6）。公開鍵サーバ 1 4 0 3 はコンピュータ B 1 4 0 4 の公開鍵問い合わせに基づき、コンピュータ A 1 4 0 2 の公開鍵をコンピュータ B 1 4 0 4 に渡す（1 5 0 7）。コンピュータ B 1 4 0 4 はコンピュータ A 1 4 0 2 の公開鍵を用いてモンゴメリ型楕円曲線を利用して暗号化を行ない、コンピュータ A に暗号化通信を行なう（ステップ 1 5 0 8）。

図 1 6 はモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムの第 5 実施例を示す図である。

曲線パラメタ生成サーバ 1 6 0 1 は第 1 実施例におけるモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を行なう楕円曲線パラメタ生成装置 1 0 1 を組み込んだサーバである。コンピュータ A 1 6 0 2 はモンゴメリ型楕円曲線を利用した楕円暗号により暗号化通信を行なうための秘密鍵公開鍵の組の生成を行なおうとしているコンピュータである。公開鍵サーバ 1 6 0 3 は各コンピュータの公開鍵の登録を行ない、問い合わせがあれば問い合わせ対象のコンピュータの公開鍵を送信する。コンピュータ B 1 6 0 4 はコンピュータ A 1 6 0

2へモンゴメリ型楕円曲線を利用して楕円暗号により暗号化通信を行な
おうとしているコンピュータである。曲線パラメタ変換装置1605は
モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を与えるとその標準
型楕円曲線に対応するモンゴメリ型楕円曲線及び標準型楕円曲線上の位
5 数2の点でモンゴメリ型楕円曲線上の点 $(0,0)$ に対応する点の x 座標を出
力するパラメタ変換装置である。

第5実施例における楕円暗号システムでは以下の手順により楕円曲
線パラメタ生成装置を利用して暗号化通信を行なう。図17はそのフ
ローチャートである。コンピュータA1602は曲線パラメタ生成サー
10 バ1601にモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型
楕円曲線の生成を要請する(ステップ1701)。曲線パラメタ生成
サーバ1601は上記曲線の生成要請に基づき、定義体情報103を楕
円曲線パラメタ生成装置101に与えて曲線パラメタ108を生成する
(ステップ1702)。ここで定義体情報103は図27における、定
15 義体のビット長を含んだ定義体情報2701もしくは定義体素数を含ん
だ定義体情報2704で与えられている。新規曲線パラメタとして、モ
ンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式及び曲線位数
をコンピュータA1602に渡す(ステップ1703)。コンピュータ
A1602は曲線パラメタ変換装置1605にモンゴメリ型楕円曲線に
20 変換可能な標準型楕円曲線の定義式を与え、曲線パラメタ変換装置から
モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を変換したモンゴメ
リ型楕円曲線の定義式及び標準型楕円曲線上の位数2の点でモンゴメリ
型楕円曲線上の点 $(0,0)$ に対応する点の x 座標を受け取る(ステップ17
04)。コンピュータA1602は上記曲線パラメタから秘密鍵公開鍵
25 の組を作成する(ステップ1705)。コンピュータA1602は公開
鍵サーバ1603に上記作成した公開鍵を登録する(ステップ170

6)。コンピュータB 1 6 0 4は公開鍵サーバ1 6 0 3にコンピュータA 1 6 0 2の公開鍵の問い合わせを行なう（ステップ1 7 0 7）。公開鍵サーバ1 6 0 3はコンピュータB 1 6 0 4の公開鍵問い合わせに基づき、コンピュータA 1 6 0 2の公開鍵をコンピュータB 1 6 0 4に渡す（ステップ1 7 0 8）。コンピュータB 1 6 0 4はコンピュータA 1 6 0 2の公開鍵を用いてモンゴメリ型楕円曲線を利用して暗号化を行ない、コンピュータAに暗号化通信を行なう（ステップ1 7 0 9）。

図1 8はモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムの第6実施例を示す図である。

曲線パラメタ生成サーバ1 8 0 1は第1実施例におけるモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を行なう楕円曲線パラメタ生成装置1 0 1を組み込んだサーバである。コンピュータA 1 8 0 2はモンゴメリ型楕円曲線を利用した楕円暗号により暗号化通信を行なうための秘密鍵公開鍵の組の生成を行なおうとしているコンピュータである。公開鍵サーバ1 8 0 3は各コンピュータの公開鍵の登録を行ない、問い合わせがあれば問い合わせ対象のコンピュータの公開鍵を送信する。コンピュータB 1 8 0 4はコンピュータA 1 8 0 2へモンゴメリ型楕円曲線を利用して楕円暗号により暗号化通信を行なおうとしているコンピュータである。曲線パラメタ変換装置1 8 0 5はモンゴメリ型楕円曲線に変換可能な標準型楕円曲線を与えるとその標準型楕円曲線に対応するモンゴメリ型楕円曲線及び標準型楕円曲線上の位数2の点でモンゴメリ型楕円曲線上の点 $(0,0)$ に対応する点の x 座標を出力するパラメタ変換装置である。

第6実施例における楕円暗号システムでは以下の手順により楕円曲線パラメタ生成装置を利用して暗号化通信を行なう。図1 9はそのフ

ローチャートである。コンピュータA1802は曲線パラメタ生成サーバ1801にモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を要請する（ステップ1901）。曲線パラメタ生成サーバ1801は上記曲線の生成要請に基づき、定義体情報103を楕円曲線パラメタ生成装置101に与えて曲線パラメタ108を生成する（ステップ1902）。ここで定義体情報103は図27における、定義体のビット長を含んだ定義体情報2701もしくは定義体素数を含んだ定義体情報2704で与えられている。新規曲線パラメタとして、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式及び曲線位数をコンピュータA1802に渡す（ステップ1903）。コンピュータA1802は上記曲線パラメタから秘密鍵公開鍵の組を作成する（ステップ1904）。コンピュータAは公開鍵サーバ1803に上記作成した公開鍵を登録する（ステップ1905）。公開鍵サーバ1803は曲線パラメタ変換装置1805にコンピュータA1802の公開鍵に関するモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式を与え、曲線パラメタ変換装置から上記モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を変換したモンゴメリ型楕円曲線の定義式及び標準型楕円曲線上の位数2の点でモンゴメリ型楕円曲線上の点 $(0,0)$ に対応する点の x 座標を受け取り、コンピュータA1802の公開鍵の情報として加える（ステップ1906）。コンピュータB1804は公開鍵サーバ1803にコンピュータA1802の公開鍵の問い合わせを行なう（ステップ1907）。公開鍵サーバ1803はコンピュータB1804の公開鍵問い合わせに基づき、コンピュータA1802の公開鍵をコンピュータB1804に渡す（ステップ1908）。コンピュータB1804はコンピュータA1802の公開鍵を用いてモンゴメリ型楕円曲線を利用して暗号化を行ない、コンピュータA1802に暗号化通信を行なう（ス

5 テップ1909)。尚、ステップ1906とステップ1907は、その
順番を問わず、コンピュータB1804が公開鍵サーバ1803にコン
ピュータA1802の公開鍵を問い合わせた後に、公開鍵サーバ180
3が曲線パラメタ変換装置1805に標準型楕円曲線をモンゴメリ型楕
円曲線に変換するよう要請しても良い。

図20はモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムの第7実施例を示す図である。

10 曲線パラメタ生成サーバ2001は第1実施例におけるモンゴメリ
型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成を行なう
楕円曲線パラメタ生成装置101を組み込んだサーバである。コン
ピュータA2002はモンゴメリ型楕円曲線を利用した楕円暗号により
暗号化通信を行なうための秘密鍵公開鍵の組の生成を行なおうとしてい
るコンピュータである。公開鍵サーバ2003は各コンピュータの公開
15 鍵の登録を行ない、問い合わせがあれば問い合わせ対象のコンピュータ
の公開鍵を送信する。コンピュータB2004はコンピュータA2002
へモンゴメリ型楕円曲線を利用して楕円暗号により暗号化通信を行な
おうとしているコンピュータである。曲線パラメタ変換装置2005は
モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を与えるとその標準
20 型楕円曲線に対応するモンゴメリ型楕円曲線及び標準型楕円曲線上の位
数2の点でモンゴメリ型楕円曲線上の点 $(0,0)$ に対応する点の x 座標を出
力するパラメタ変換装置である。

第7実施例における楕円暗号システムでは以下の手順により楕円曲
線パラメタ生成装置を利用して暗号化通信を行なう。図21はそのフ
ローチャートである。コンピュータA2002は曲線パラメタ生成サー
25 バ2001にモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型

楕円曲線の生成を要請する（ステップ2101）。曲線パラメタ生成サーバ2001は上記曲線の生成要請に基づき、定義体情報103を楕円曲線パラメタ生成装置101に与えて曲線パラメタ108を生成する（ステップ2102）。ここで定義体情報103は図27における、定義体のビット長を含んだ定義体情報2701もしくは定義体素数を含んだ定義体情報2704で与えられている。新規曲線パラメタとして、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式及び曲線位数をコンピュータA2002に渡す（ステップ2103）。コンピュータA2002は上記曲線パラメタから秘密鍵公開鍵の組を作成する（ステップ2104）。コンピュータA2002は公開鍵サーバ2003に上記作成した公開鍵を登録する（ステップ2105）。コンピュータB2004は公開鍵サーバ2003にコンピュータA2002の公開鍵の問い合わせを行なう（ステップ2106）。公開鍵サーバ2003はコンピュータB2004の公開鍵問い合わせに基づき、コンピュータA2002の公開鍵をコンピュータB2004に渡す（ステップ2107）。コンピュータBは曲線パラメタ変換装置2005にコンピュータA2002の公開鍵に関するモンゴメリ型楕円曲線に変換可能な標準型楕円曲線の定義式を与え、曲線パラメタ変換装置から上記モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を変換したモンゴメリ型楕円曲線の定義式及び標準型楕円曲線上の位数2の点でモンゴメリ型楕円曲線上の点(0,0)に対応する点のx座標を受け取り、コンピュータA2002の公開鍵の情報として加える（ステップ2108）。コンピュータB2004はコンピュータA2002の公開鍵を用いてモンゴメリ型楕円曲線を利用して暗号化を行ない、コンピュータAに暗号化通信を行なう（ステップ2109）。

図22はモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型

楕円曲線の生成装置における標準型楕円曲線からモンゴメリ型楕円曲線への変換可能判定を行なう変換可能判定装置の一実施例を示す図である。

変換可能判定装置 2 2 0 1 は根存在判定部 2 2 0 2 及び平方剰余判定部 2 2 0 3 を用いて与えられた標準型楕円曲線がモンゴメリ型楕円曲線
5 に変換可能であるかを判定する。根存在判定部 2 2 0 2 では $f(x)=0$ が F_p において根を持つか判定する。平方剰余判定部 2 2 0 3 で $f'(\alpha)$ が平方非剰余であると判定された根以外に根が存在しなければ変換不可能と出力する。根が存在すれば根を平方剰余判定部 2 2 0 3 に与える。平方剰余判定部 2 2 0 3 では $f(\alpha)=0$ となる α に対して、 $f'(\alpha)$ が F_p において平方剰余であるかを判定する。平方剰余であれば変換可能と出力する。
10 平方非剰余であれば根存在判定部に他の根が存在するかを問い合わせる。

変換可能判定装置 2 2 0 1 では以下の手順により、標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かを判定する。図 3 のフローチャートを用いて説明する。ステップ 3 0 1 において標準型楕円曲線
15 $y^2 = f(x) = x^3 + ax + b$ に対して $f(\alpha)=0$ となる F_p の元 α が存在するかを調べる。そのような元 α が存在しなければ変換不可能 3 0 4 と出力し終了する。上記 α が存在すれば、ステップ 3 0 2 により、 $f(\alpha)=0$ となる α に対して、平方剰余判定部 2 2 0 3 により $f'(\alpha)$ が F_p において平方剰余かを判定し、その結果が平方剰余となる α が存在するかを判定する。そのような
20 α が存在すれば変換可能 3 0 3 と出力し終了する。そのような α が存在しなければ変換不可能 3 0 4 と出力して終了する。

図 2 3 は図 1 6、図 1 8、図 2 0 のモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムにおける曲線パラメタ変換装置の一実施例を示す図である。

25 曲線パラメタ変換装置 2 3 0 1 は根計算部 2 3 0 3、平方剰余判定部 2 3 0 2 及び曲線パラメタ構成部 2 3 0 4 を用いて、与えられたモン

ゴメリ型楕円曲線に変換可能な標準型楕円曲線から対応するモンゴメリ型楕円曲線及び点変換パラメタとして標準型楕円曲線上の位数2の点でモンゴメリ型楕円曲線上の点 $(0,0)$ に対応する点の x 座標を計算し出力する。根計算部2303では $f(x)=0$ の F_p における根 α を求める。平方剰余判定部2302では根計算部2303で求めた α に対して、 $f'(\alpha)$ が F_p において平方剰余であるかを判定する。曲線パラメタ構成部2304では根計算部2303で求めた α からモンゴメリ型楕円曲線を構成する。

曲線パラメタ変換装置2301では以下の手順により、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線から変換されたモンゴメリ型楕円曲線及び標準型楕円曲線上の位数2の点でモンゴメリ型楕円曲線上の点 $(0,0)$ に対応する点の x 座標を計算する。図24のフローチャートを用いて説明する。ステップ2401により、 $f(x)=0$ の F_p における根 α を求める。ステップ2403において $f'(\alpha)$ が F_p において平方剰余であるかを判定する。平方剰余であればステップ2404へ行く。平方非剰余であれば、ステップ2402により $f(x)=0$ の根でステップ2403で $f'(\alpha)$ が平方非剰余と分かった根 α 以外の根を求める。その根を新たに α とする。その α に対して再度ステップ2403で $f'(\alpha)$ が F_p において平方剰余であるかを判定する。 $f(x)=0$ の根は高々3個しかなく、またモンゴメリ型楕円曲線に変換可能であることが分かっているので、3回繰り返すうちに $f'(\alpha)$ が平方剰余と判定されステップ2404へ進む。ステップ2404において、 $s=f'(\alpha)^{-1/2}$ を計算する。ステップ2405において、 $B=s, A=3as$ を計算する。ステップ2406において、 A, B, α を出力する。

このような曲線パラメタ変換装置により、図27の標準型楕円曲線のみで与えられた曲線パラメタ2702に対応するモンゴメリ型楕円曲

線のデータを付け加えた曲線パラメタ 2 7 0 5 に、標準型楕円曲線のみ
 で与えられた公開鍵 2 7 0 3 を対応するモンゴメリ型楕円曲線のデータ
 を付け加えた公開鍵 2 7 0 6 に変換できる。

図 2 5 は F_p の拡大体 F_q 上定義された、モンゴメリ型楕円曲線に変換
 5 可能であり且つ安全な標準型楕円曲線の生成装置における標準型楕円曲
 線からモンゴメリ型楕円曲線への変換可能判定を行なう変換可能判定装
 置の一実施例を示す図である。

変換可能判定装置 2 5 0 1 は根存在判定部 2 5 0 2 及び平方根判定
 部 2 5 0 3 を用いて、与えられた F_q 上定義された標準型楕円曲線がモ
 10 ンゴメリ型楕円曲線に変換可能であることを判定する。根存在判定部 2 5
 0 2 では $f(x)=0$ が F_q において根を持つかを判定する。平方根判定部 2 5
 0 3 で $f'(\alpha)$ が平方非剰余であると判定された根以外に根が存在しなけ
 れば変換不可能と出力する。根が存在すれば根を平方根判定部 2 5 0 3
 に与える。平方根判定部 2 5 0 3 では $f(\alpha)=0$ となる α に対して、
 15 $f'(\alpha)$ が F_q において平方根を持つかを判定する。平方根を持てば変換可
 能と出力する。平方根を持たなければ根存在判定部に $f(x)=0$ の他の根
 が存在するかを問い合わせる。

変換可能判定装置 2 5 0 1 では以下の手順により、 F_q 上定義された
 標準型楕円曲線がモンゴメリ型楕円曲線に変換可能かを判定する。図 2
 20 6 のフローチャートを用いて説明する。ステップ 2 6 0 1 において標準
 型楕円曲線 $y^2 = f(x) = x^3 + ax + b$ に対して $f(\alpha)=0$ となる F_q の元 α が存在
 するかを調べる。そのような元 α が存在しなければ変換不可能 2 6 0 4
 と出力し終了する。上記 α が存在すれば、ステップ 2 6 0 2 により、
 $f(\alpha)=0$ となる α に対して、平方根判定部 2 5 0 3 により $f'(\alpha)$ が F_q に
 25 において平方根を持つかを判定し、その結果が平方根を持つ α が存在する
 かを判定する。そのような α が存在すれば変換可能 2 6 0 3 と出力し終

了する。そのような α が存在しなければ変換不可能 2 6 0 4 と出力して終了する。

図 2 8 はモンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成装置を組み込んだ楕円暗号システムにおいて公開鍵サーバ、コンピュータ A 乃至はコンピュータ B に組み込むための曲線置換管理装置の実施例を示す図である。

曲線置換管理装置 2 8 0 1 は、判定曲線選択部 2 8 0 2、曲線置換判定部 2 8 0 3 及び鍵テーブル 2 8 0 4 を含む。鍵テーブル 2 8 0 4 は曲線パラメタ及び公開鍵を含むデータテーブルである。

判定曲線選択部 2 8 0 2 は指定時間もしくは一定時間毎に起動し、鍵テーブル 2 8 0 4 より曲線パラメタを選択する。選択した曲線パラメタを曲線置換判定部 2 8 0 3 に送る。曲線置換判定部 2 8 0 3 は受け取った曲線パラメタに対して、曲線パラメタが作成された時間もしくはその曲線パラメタの利用者の数が、それぞれ安全性を保つために必要となる値よりも古いもしくは多い時に、与えられた曲線パラメタを新規の曲線パラメタに置換する必要があると出力する。

図 2 9 は図 2 8 の曲線置換管理装置を公開鍵サーバに組み込んだ場合における処理の流れを示すシーケンス図である。

曲線置換管理装置 2 9 0 3 は曲線パラメタ置換要請を公開鍵サーバ 2 9 0 2 に送る。公開鍵サーバ 2 9 0 2 は曲線置換管理装置 2 9 0 3 からの曲線パラメタ置換要請に基づき、曲線パラメタ生成要請を曲線パラメタ生成サーバ 2 9 0 1 に送る。曲線パラメタ生成サーバ 2 9 0 1 は公開鍵サーバ 2 9 0 2 からの曲線パラメタ生成要請に基づき、新規曲線パラメタを生成し、新規曲線パラメタを公開鍵サーバ 2 9 0 2 に送る。公開鍵サーバ 2 9 0 2 は曲線パラメタを曲線パラメタ生成サーバ 2 9 0 1 から受け取った新規曲線パラメタに置き換える。公開鍵サーバ 2 9 0 2

は、以前の曲線パラメタを利用しているコンピュータ A 2 9 0 4 に、新規曲線パラメタとともに新規公開鍵登録要請を送る。コンピュータ A 2 9 0 4 は、公開鍵サーバ 2 9 0 2 からの新規公開鍵登録要請に基づき、受け取った新規曲線パラメタに対する秘密鍵公開鍵の組の生成を行なう。

5 コンピュータ A 2 9 0 4 は生成した公開鍵を公開鍵サーバ 2 9 0 2 に登録する。

以上述べたように本発明によれば、モンゴメリ型楕円曲線に変換可能であり且つ安全な標準型楕円曲線の生成において、安全な標準型楕円曲線の再生成を省くことができるので、上記性質を持った楕円曲線の生成にかかるコストを削減できる。暗号に利用する楕円曲線を定期的に上記性質を持つ新しい楕円曲線に置き換えることにより特定楕円曲線に対する攻撃を未然に防ぐ事ができ、さらにモンゴメリ型楕円曲線に変換可能であることからデータの暗号化復号化における時間を標準型楕円曲線を用いた場合よりも短縮することができる。

10

15

産業上の利用可能性

以上のとおり、本発明は、コンピュータネットワークにおけるセキュリティを行う上で有用であり、特に楕円暗号を用いたセキュリティ管理をおこなう環境に用いるのに適している。

請 求 の 範 囲

1. 第1の楕円曲線を生成するステップと、前記第1の楕円曲線に関連する第2の楕円曲線を生成するステップと、前記第1の楕円曲線が第3の楕円曲線に変換可能であるかを判定するステップと、前記第1の楕円曲線が前記第3の楕円曲線に変換可能である場合、前記第1の楕円曲線及び前記第2の楕円曲線の安全性を判定するステップとを有することを特徴とする楕円曲線生成方法。
2. 請求の範囲第1項記載の楕円曲線生成方法であって、前記第2の楕円曲線は前記第1の楕円曲線のツイストであることを特徴とする楕円曲線生成方法。
3. 請求の範囲第1項記載の楕円曲線生成方法であって、前記第1の楕円曲線は $y^2 = x^3 + ax + b$ であり、前記第2の楕円曲線は $y^2 = x^3 + ar^2x + br^3$ であり、前記第3の楕円曲線は $BY^2 = X^3 + AX^2 + X$ であることを特徴とする楕円曲線生成方法。
4. 請求の範囲第3項記載の楕円曲線生成方法であって、前記第3の楕円曲線に変換可能であるかを判定するステップは、前記第1の楕円曲線 $y^2 = f(x)$ に対して、 $f(\alpha) = 0$ となる α が存在するかを判定するステップと、 $f(\alpha) = 0$ となる α に対して $f'(\alpha)$ が平方根を持つかを判定するステップとからなることを特徴とする楕円曲線生成方法。
5. 請求の範囲第1項記載の楕円曲線生成方法であって、前記第1の楕円曲線の安全性を判定するステップは、前記第1の楕円曲線の曲線位数に関する情報を抽出するステップと、前記曲線位数に関する情報からコファクタの判定を行うステップとを有することを特徴とする楕円曲線生成方法。
6. 請求の範囲第1項記載の楕円曲線生成方法であって、予め定められ

た素数位数の体上定義された第1の楕円曲線を用いることを特徴とする楕円曲線生成方法。

5 7. 第1の楕円曲線を生成するステップと、前記第1の楕円曲線が第2の楕円曲線に変換可能であるかを判定するステップと、前記第1の楕円曲線が前記第2の楕円曲線に変換可能である場合、前記第1の楕円曲線の安全性を判定するステップと、前記第1の楕円曲線が安全でないと判定された場合、前記第1の楕円曲線に付随する第3の楕円曲線の安全性を判定するステップとを有することを特徴とする楕円曲線生成方法。

10 8. 楕円暗号における楕円曲線の生成方法であって、ランダムな標準型楕円曲線 $y^2 = x^3 + ax + b$ を生成するステップと、前記生成された標準型楕円曲線 $y^2 = x^3 + ax + b$ がモンゴメリ型楕円曲線 $BY^2 = X^3 + AX^2 + X$ に変換可能であるかを判定するステップと、前記楕円曲線の曲線位数の8による整除性を判定するステップと、前記楕円曲線の曲線位数に関する情報を収集するステップと、前記曲線位数の情報からコファクタの値を判定するステップとからなり、モンゴメリ型楕円曲線
15 に変換可能であり且つコファクタが4である標準型楕円曲線を生成することを特徴とする楕円曲線生成方法。

20 9. 第1の楕円曲線 $y^2 = x^3 + ax + b$ を生成する楕円曲線候補生成部と、前記第1の楕円曲線が第2の楕円曲線 $BY^2 = X^3 + AX^2 + X$ に変換可能であるかを判定する変換可能判定部と、前記第2の楕円曲線に変換可能な第1の楕円曲線の安全性を判定する安全性判定部とを備えたことを特徴とする楕円曲線生成装置。

25 10. 請求の範囲第9項記載の楕円曲線生成装置であって、前記変換可能判定部は、前記第1の楕円曲線に対して、 $f(\alpha) = 0$ となる α が存在するかを判定する根存在判定部と、 $f(\alpha) = 0$ となる α に対して $f'(\alpha)$ が平方根を持つかを判定する平方根判定部とからなることを

特徴とする楕円曲線生成装置。

1 1. 請求の範囲第9項記載の楕円曲線生成装置であって、前記変換可能判定部は、前記第1の楕円曲線に対して、 $f(\alpha) = 0$ となる α が存在するかを判定する根存在判定部と、 $f(\alpha) = 0$ となる α に対して
5 $f'(\alpha)$ が平方剰余であるかを判定する平方剰余判定部とからなることを特徴とする楕円曲線生成装置。

1 2. 第1の計算機と第2の計算機との間で暗号化通信を行う暗号システムで使用される楕円曲線生成装置であって、前記計算機から楕円曲線の生成要請を受け、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線
10 を生成することを特徴とする楕円曲線生成装置。

1 3. 楕円曲線生成方法を実行するプログラムを格納した記録媒体であって、前記楕円曲線生成方法は以下を含む：第1の楕円曲線 $y^2 = x^3 + ax + b$ を生成するステップと、前記第1の楕円曲線に関連する第2の楕円曲線 $y^2 = x^3 + ar^2x + br^3$ を生成するステップと、前記
15 第1の楕円曲線が第3の楕円曲線 $BY^2 = X^3 + AX^2 + X$ に変換可能であるかを判定するステップと、前記第3の楕円曲線に変換可能な第1の楕円曲線の安全性を判定するステップと、前記第2の楕円曲線の安全性を判定するステップ。

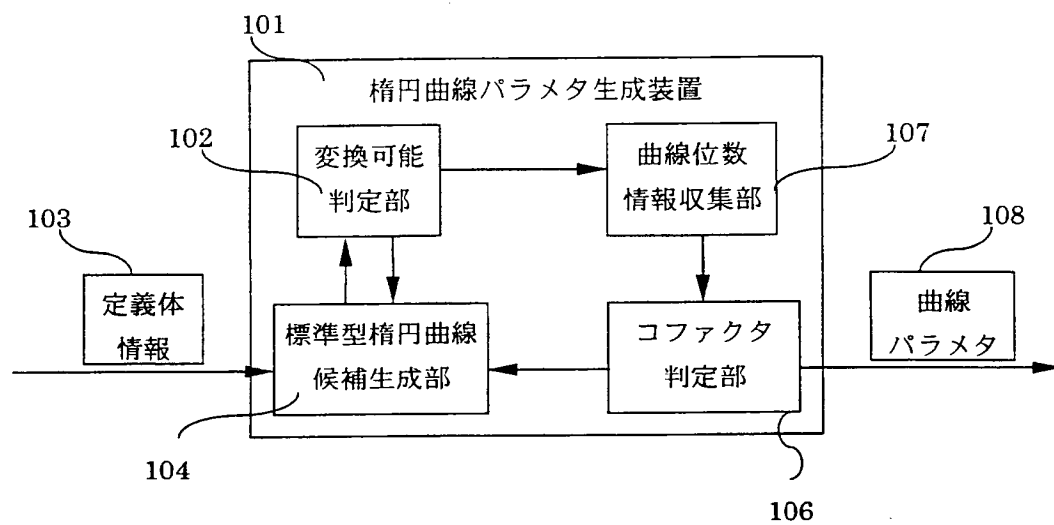
1 4. 楕円暗号を利用して暗号化通信を行う暗号システムであって、暗号化通信を受信する第1の計算機と、暗号化通信を送信する第2の計算機と、前記第1の計算機から楕円曲線の生成要請を受けて、モンゴメリ型楕円曲線に変換可能な標準型楕円曲線を生成する楕円曲線生成装置とを備えたことを特徴とする暗号システム。

1 5. 請求の範囲第14項記載の暗号システムであって、暗号化通信に使用している楕円曲線に置換の必要性があるか否かを管理する曲線置換管理装置を更に備え、前記楕円曲線に置換の必要性が生じた場合は、前
25

記楕円曲線生成装置が新たに生成した楕円曲線に置換して暗号化通信を行うことを特徴とする暗号システム。

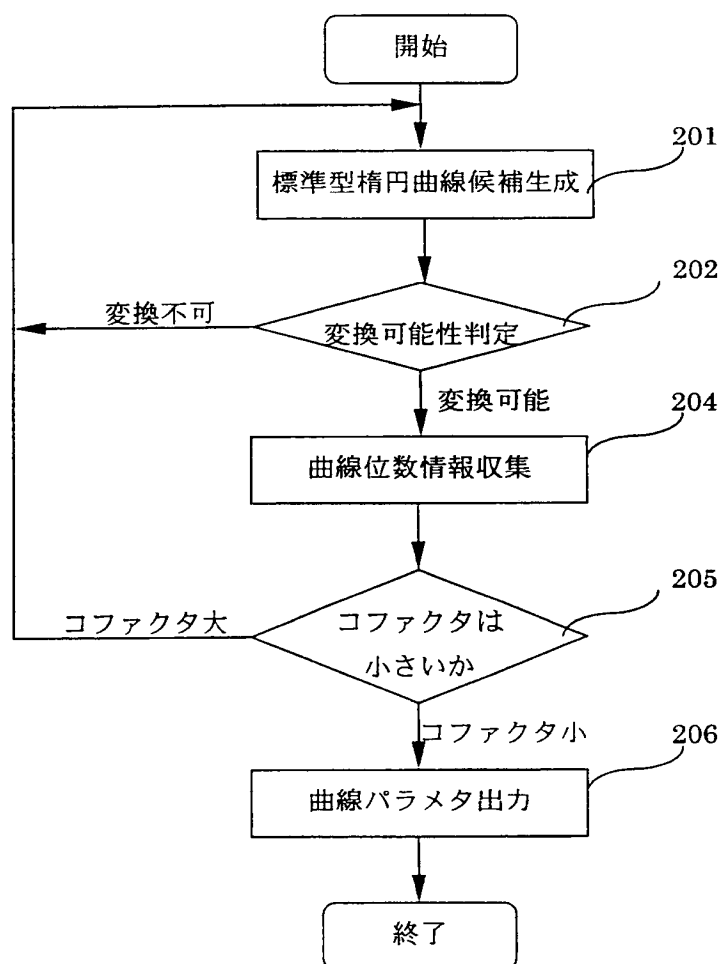
1/29

第 1 図



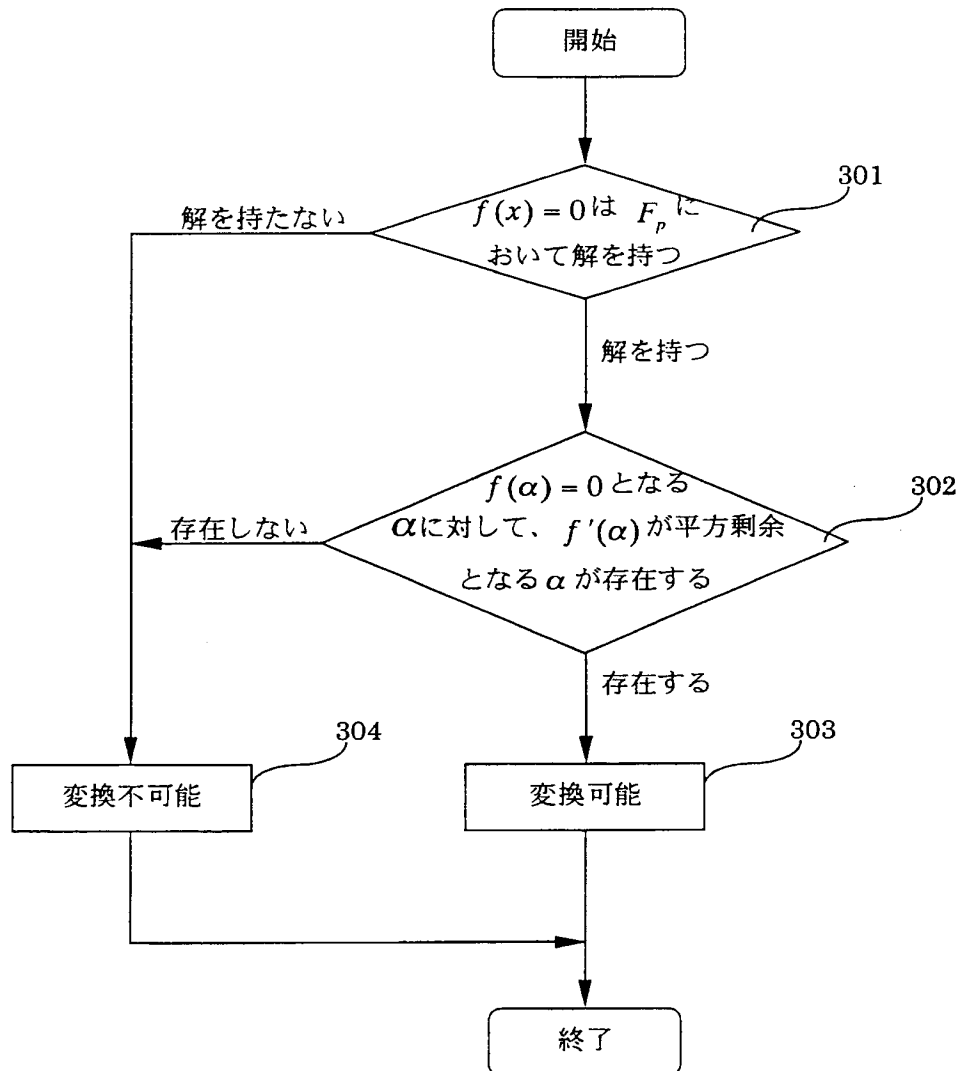
2/29

第 2 図



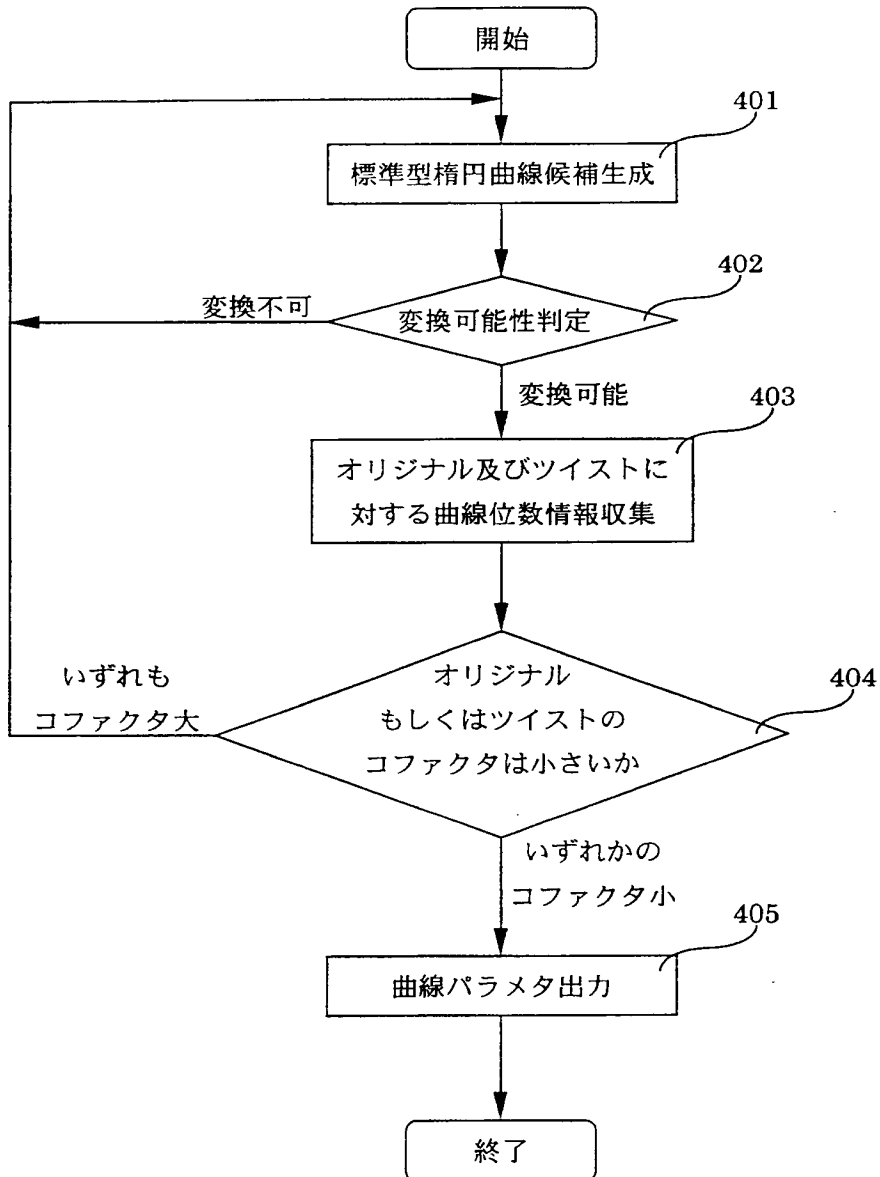
3/29

第 3 図



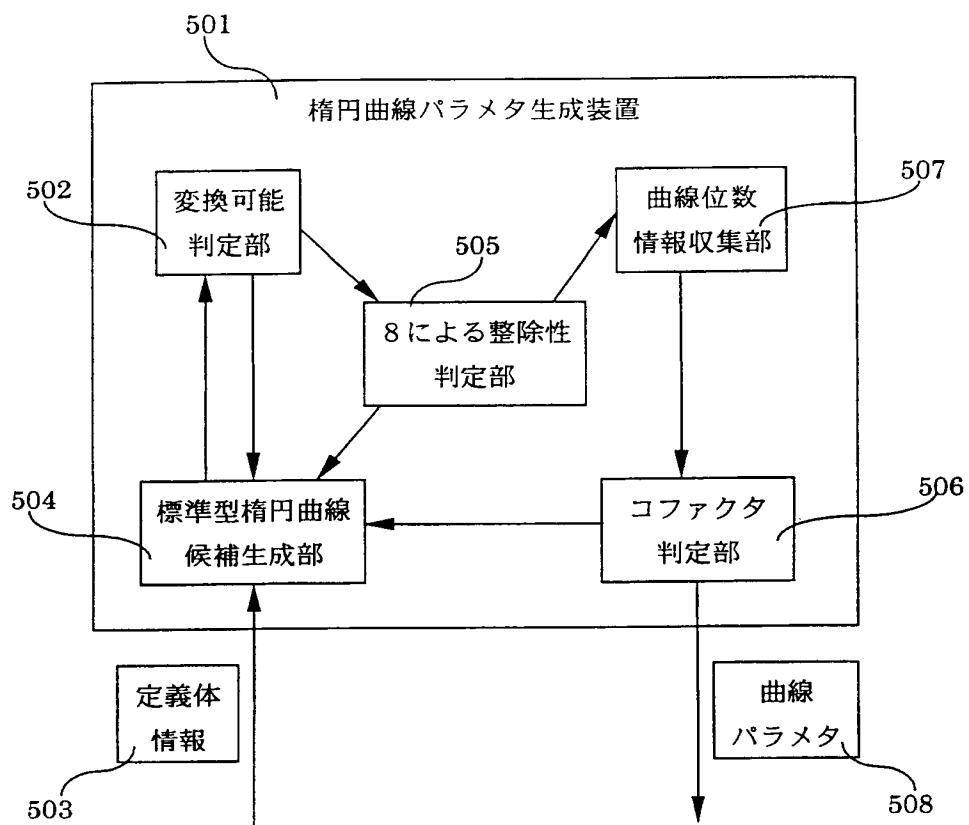
4/29

第 4 図



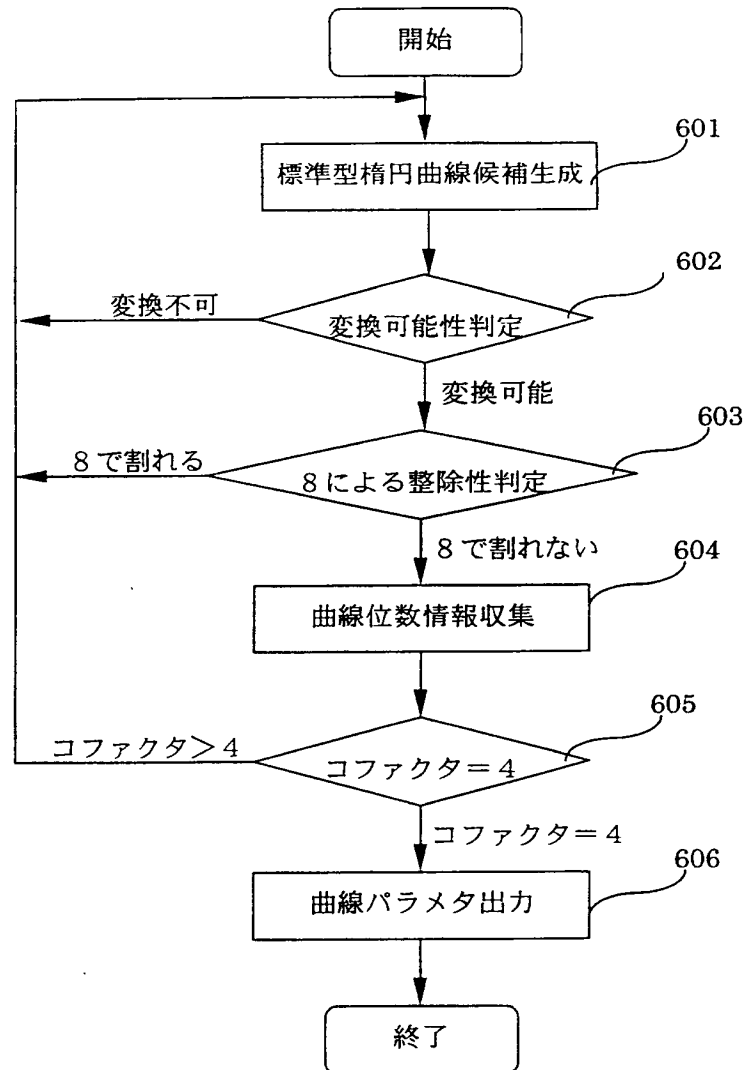
5/29

第 5 図



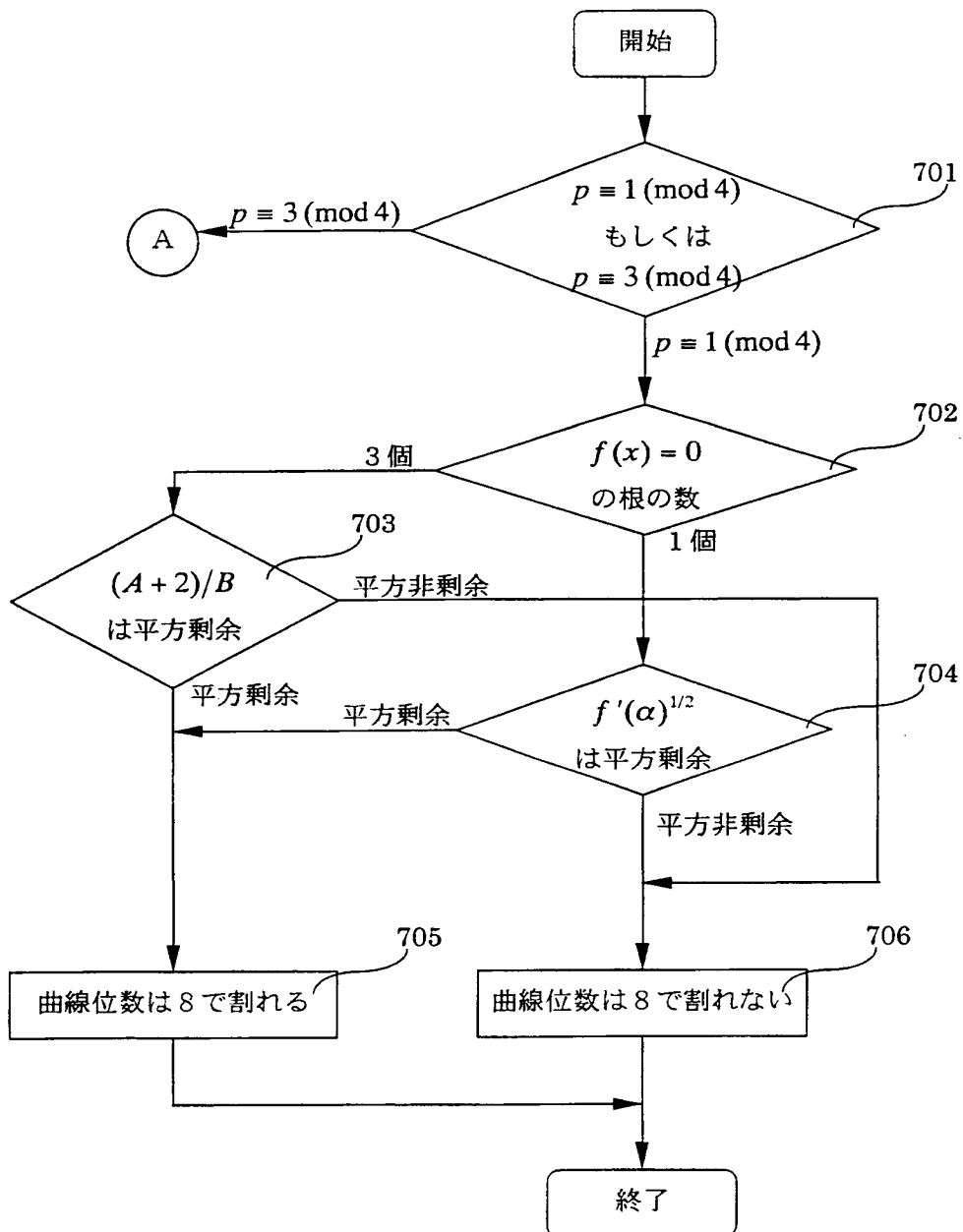
6/29

第 6 図



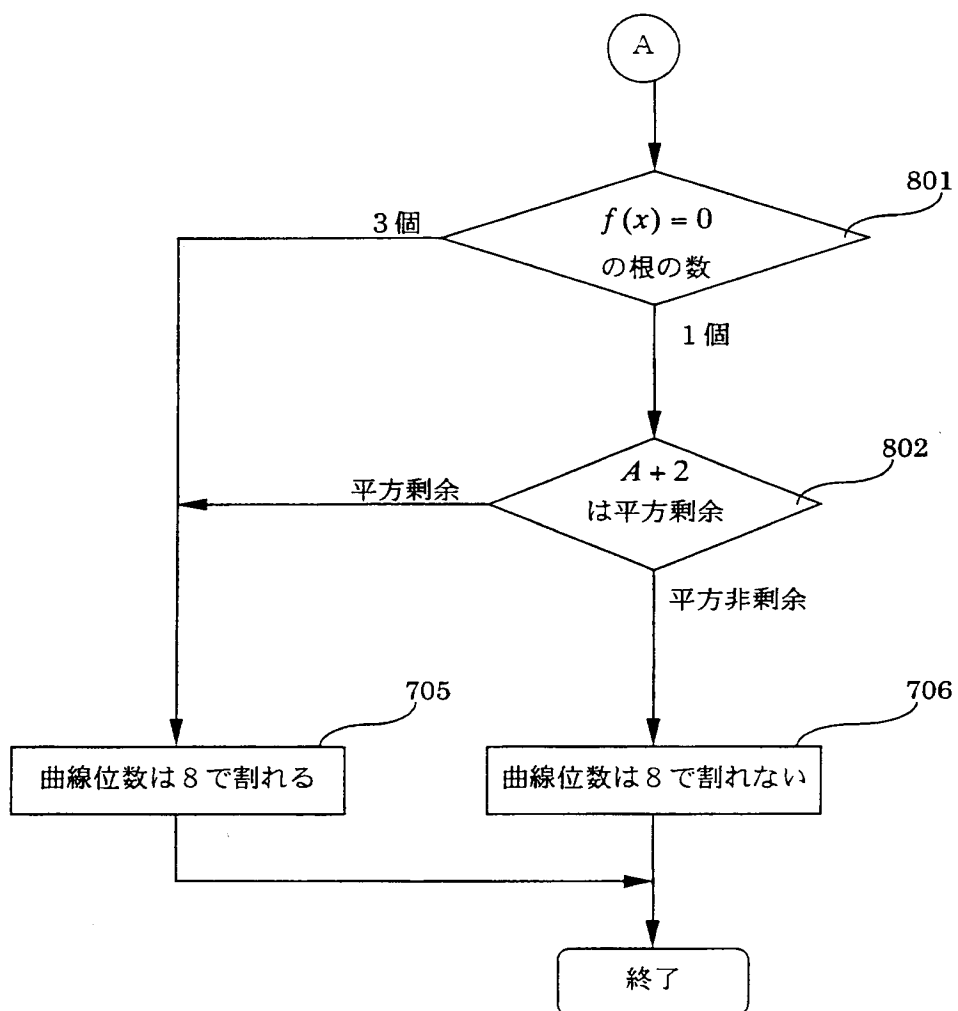
7/29

第 7 図



8/29

第 8 図



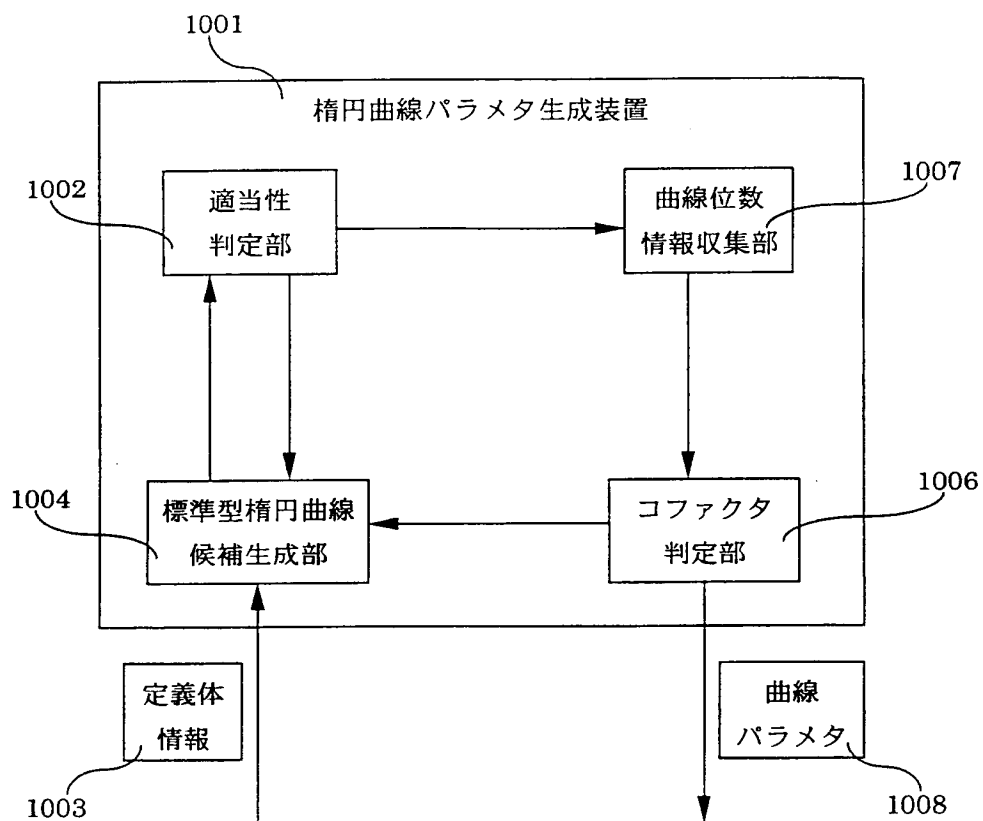
9/29

第 9 図

-1	$A+2$	$A-2$	B	曲線位数
平方剰余	平方剰余	平方非剰余	平方剰余	8 で割れる
平方剰余	平方剰余	平方非剰余	平方非剰余	8 で割れない
平方剰余	平方非剰余	平方剰余	平方剰余	8 で割れる
平方剰余	平方非剰余	平方剰余	平方非剰余	8 で割れない
平方剰余	平方剰余	平方剰余	平方剰余	8 で割れる
平方剰余	平方剰余	平方剰余	平方非剰余	8 で割れない
平方剰余	平方非剰余	平方非剰余	平方剰余	8 で割れない
平方剰余	平方非剰余	平方非剰余	平方非剰余	8 で割れる
平方非剰余	平方剰余	平方非剰余	平方剰余	8 で割れる
平方非剰余	平方剰余	平方非剰余	平方非剰余	8 で割れる
平方非剰余	平方非剰余	平方剰余	平方剰余	8 で割れない
平方非剰余	平方非剰余	平方剰余	平方非剰余	8 で割れない
平方非剰余	平方剰余	平方剰余	平方剰余	8 で割れる
平方非剰余	平方剰余	平方剰余	平方非剰余	8 で割れる
平方非剰余	平方非剰余	平方非剰余	平方剰余	8 で割れる
平方非剰余	平方非剰余	平方非剰余	平方非剰余	8 で割れる

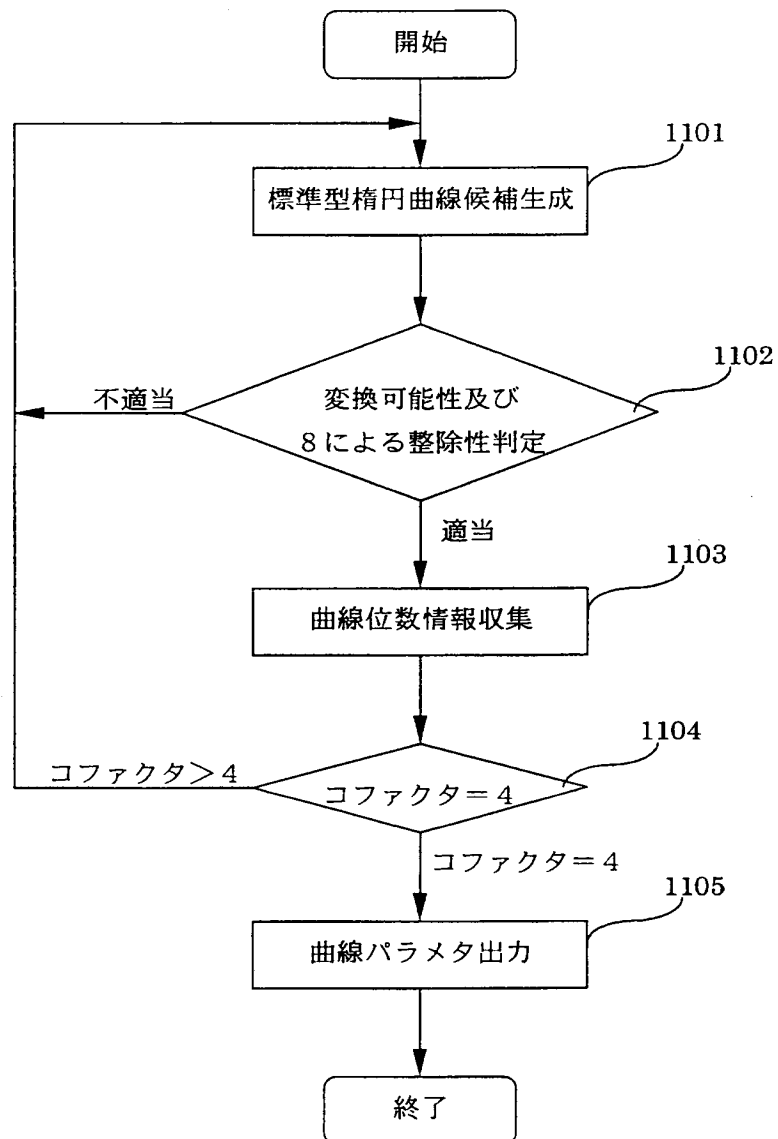
10/29

第 10 図



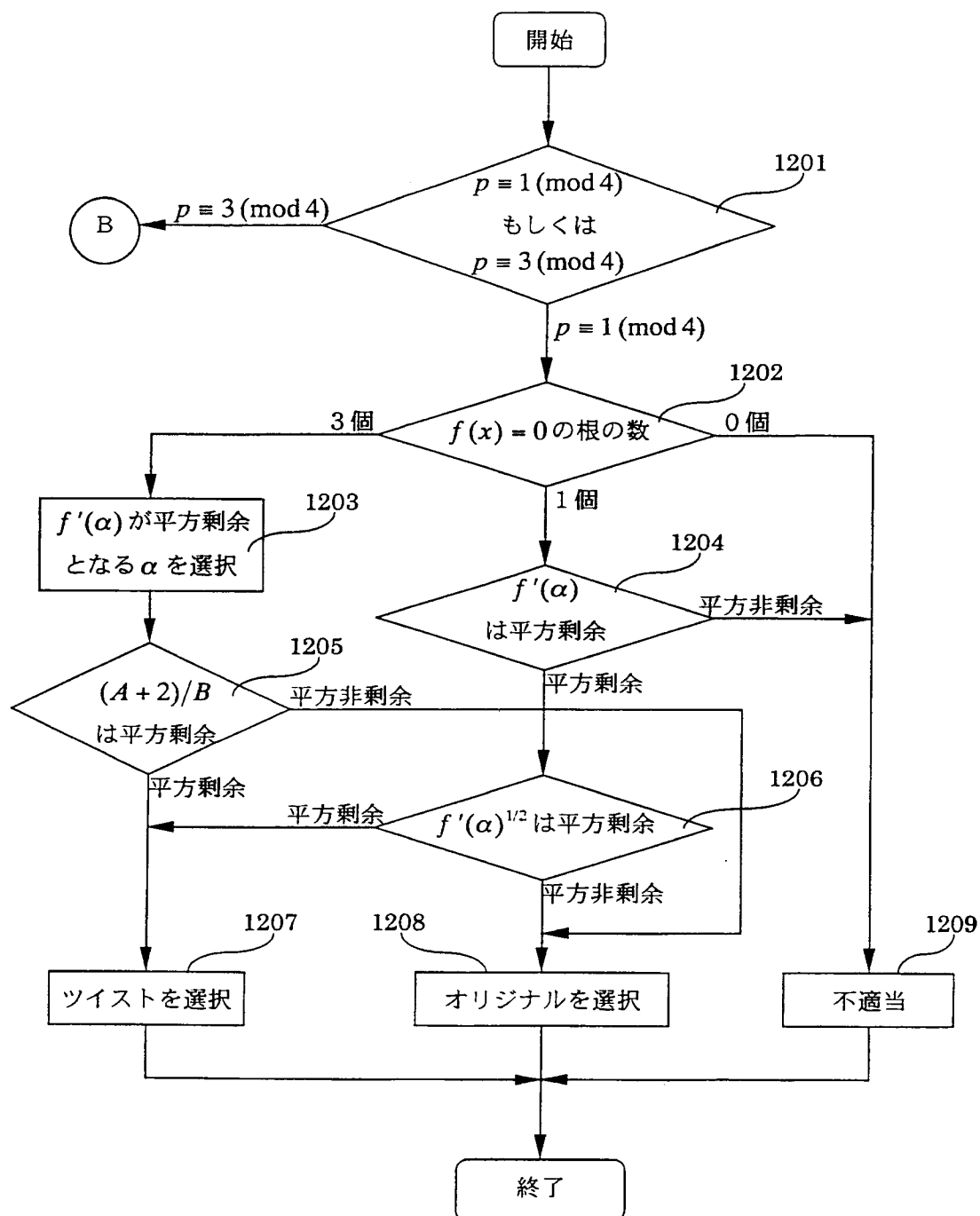
11/29

第 11 図



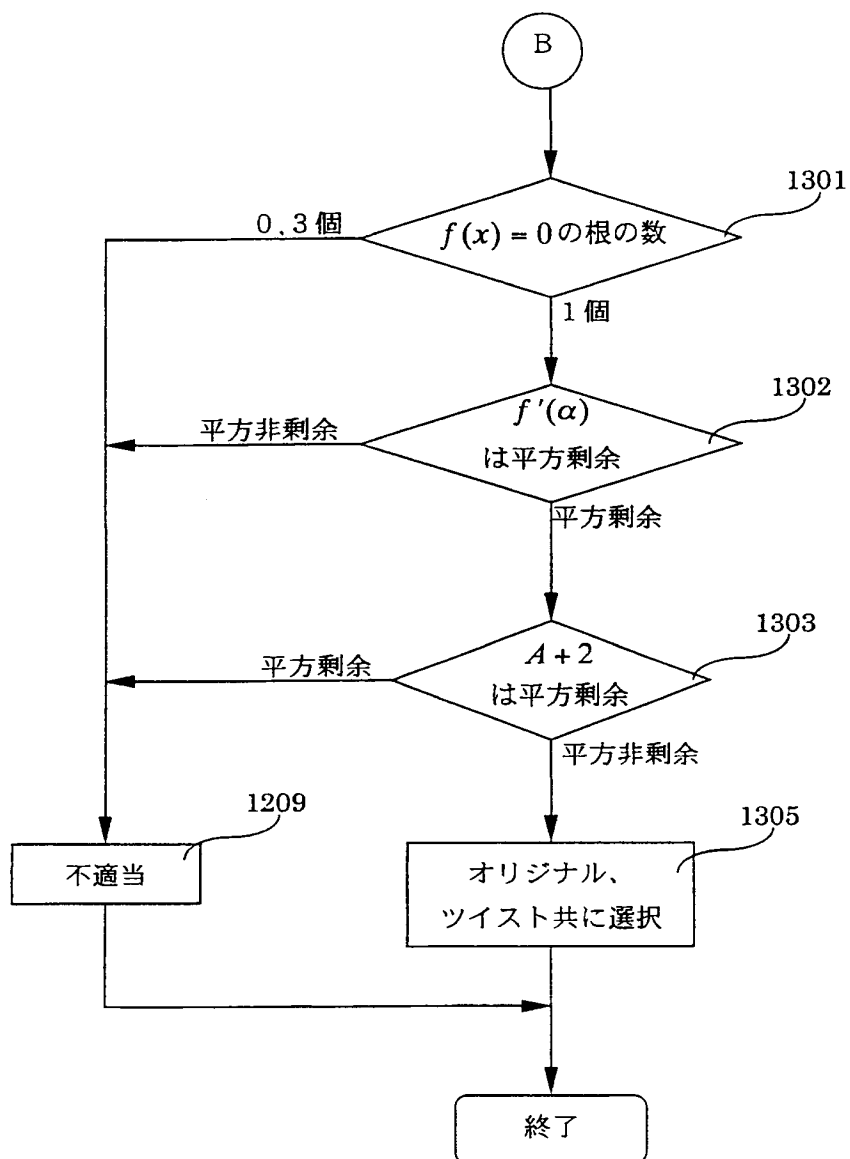
12/29

第 12 図



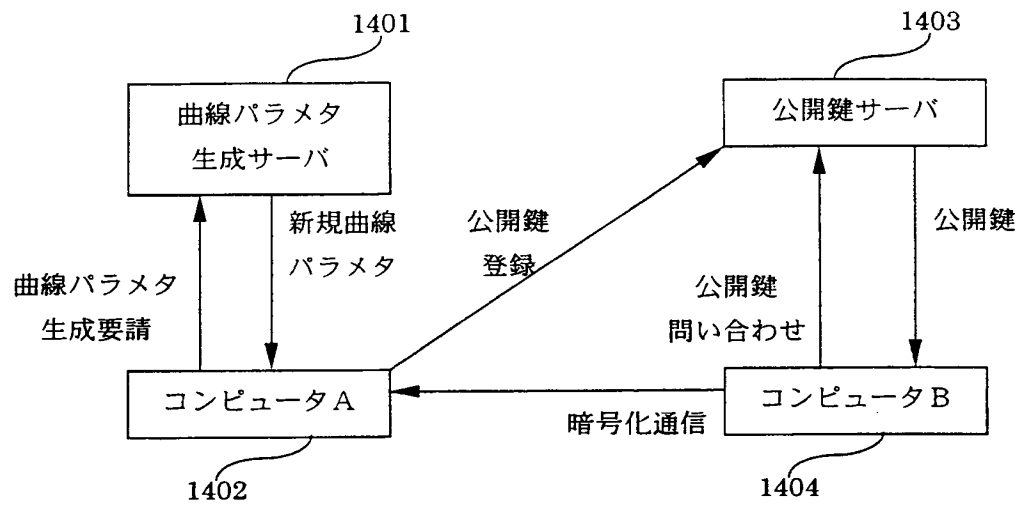
13/29

第 13 図



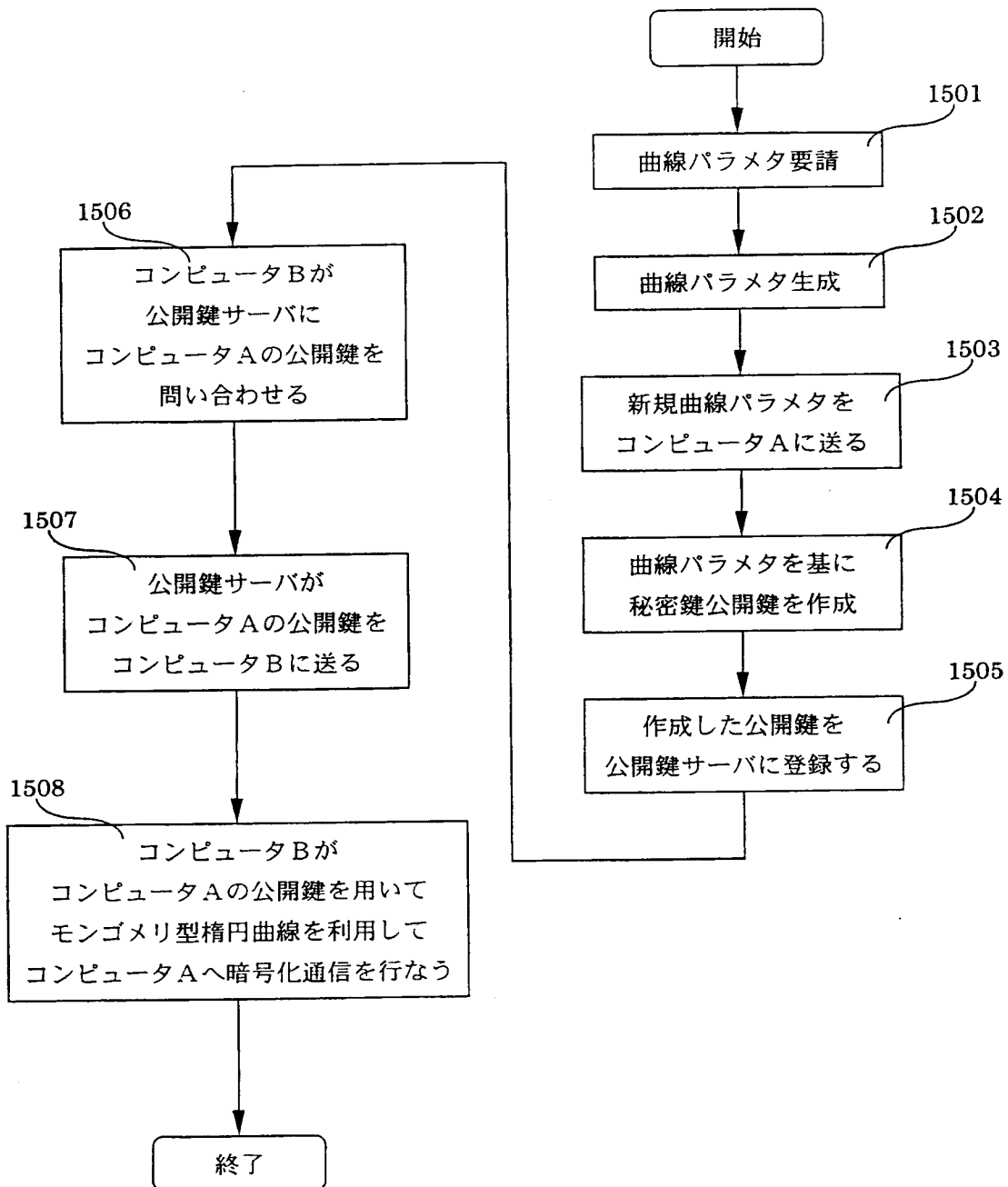
14/29

第 14 図



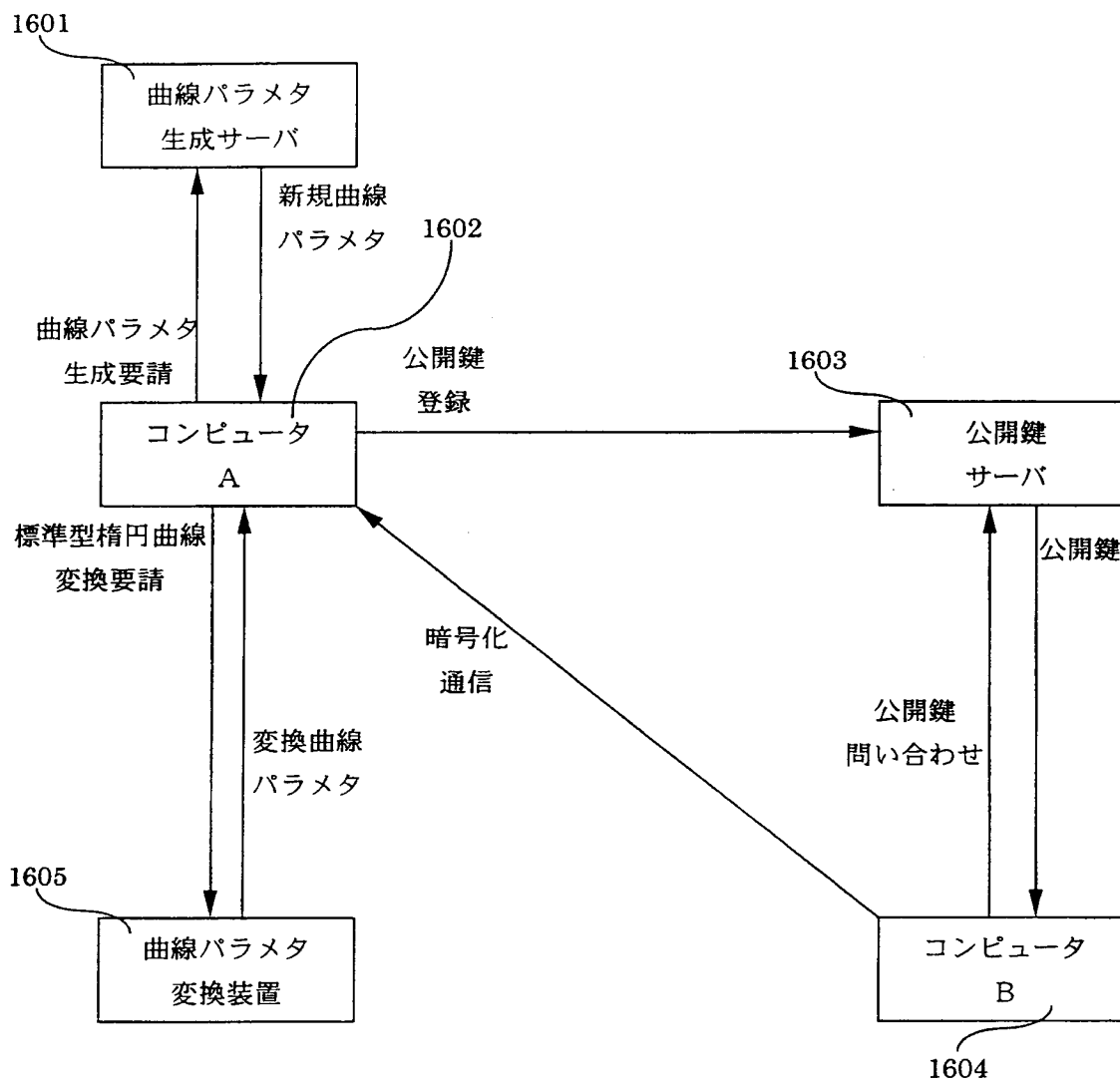
15/29

第 15 図



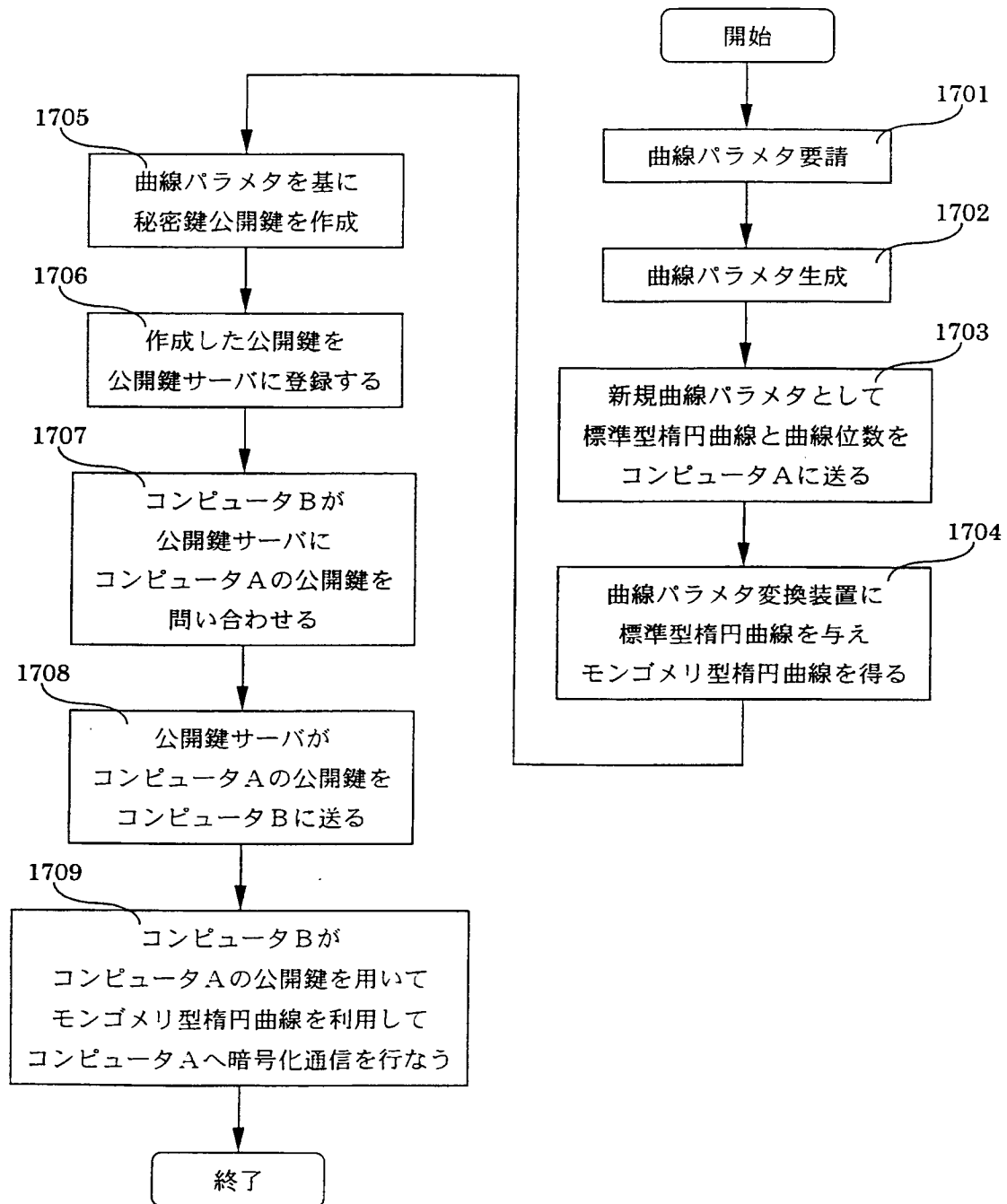
16/29

第 16 図



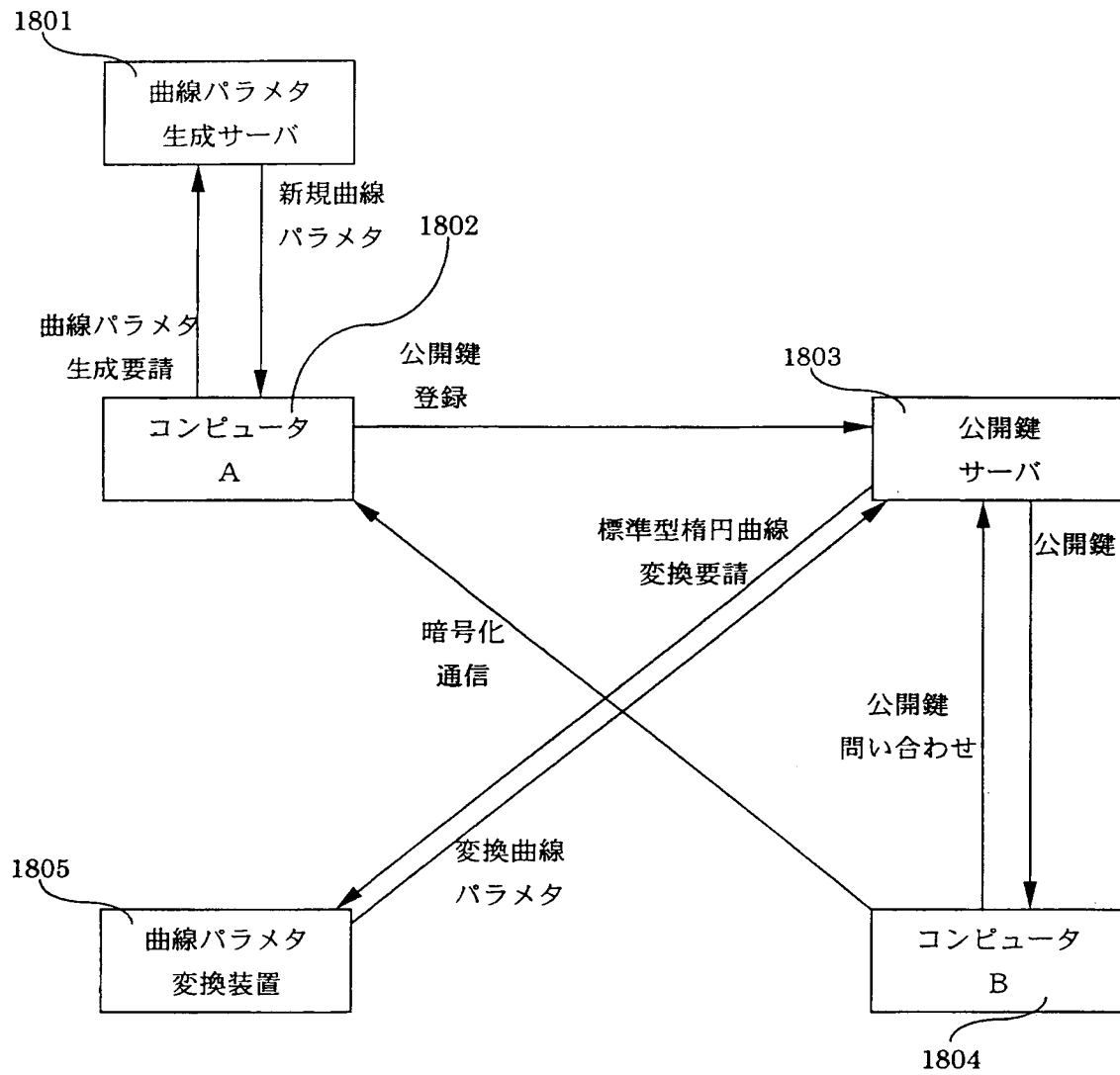
17/29

第 17 図



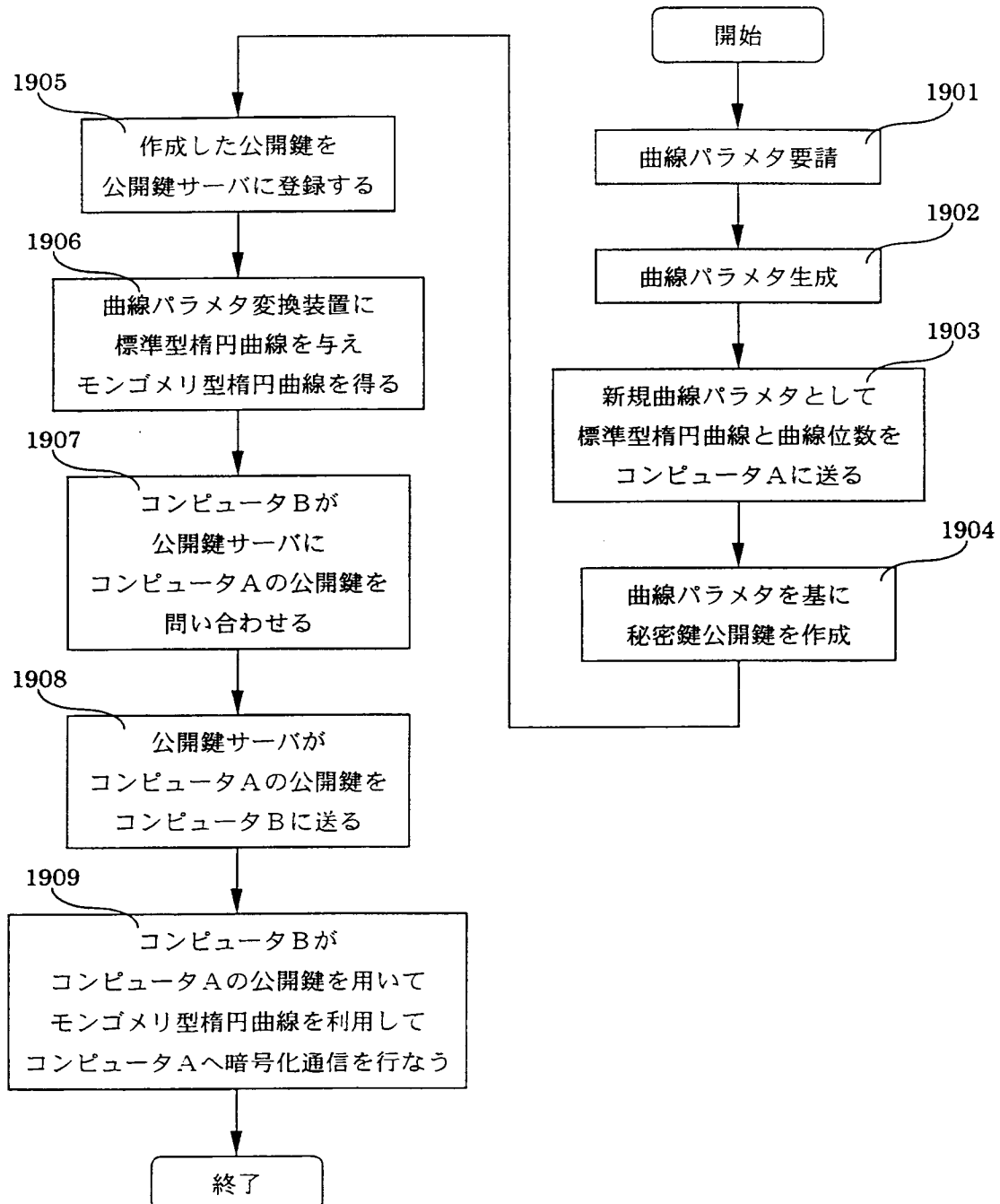
18/29

第 18 図



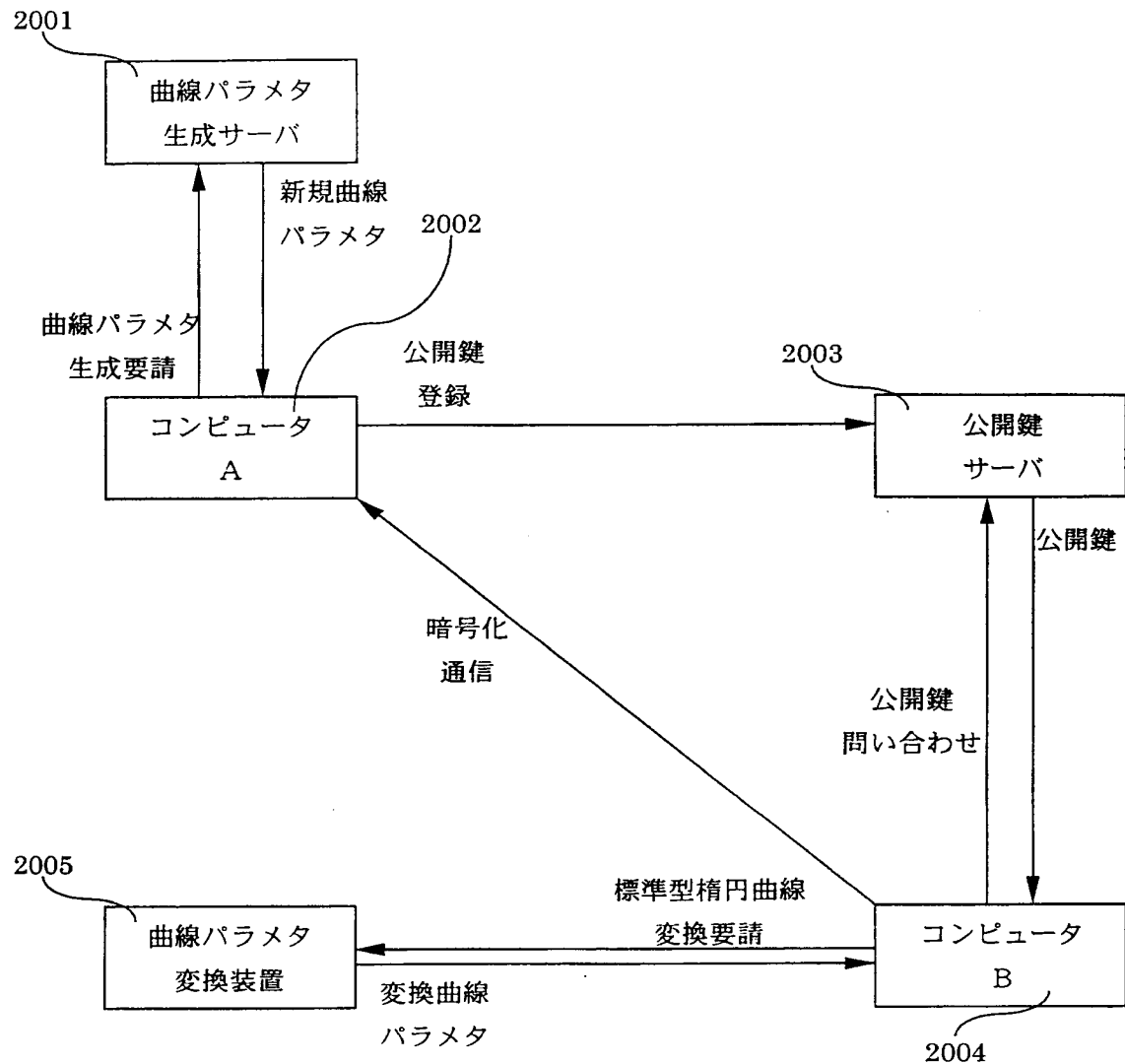
19/29

第 19 図



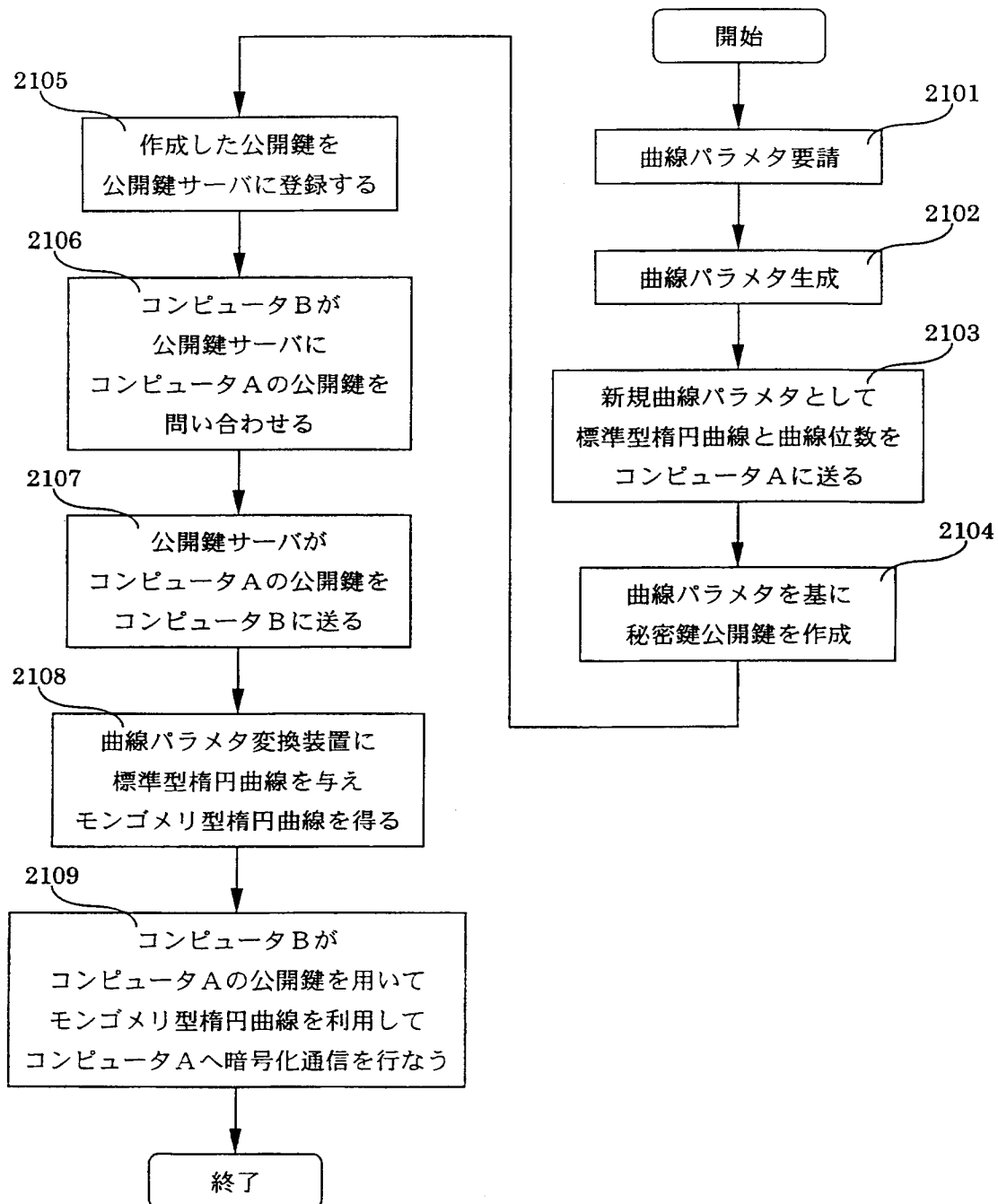
20/29

第 20 図



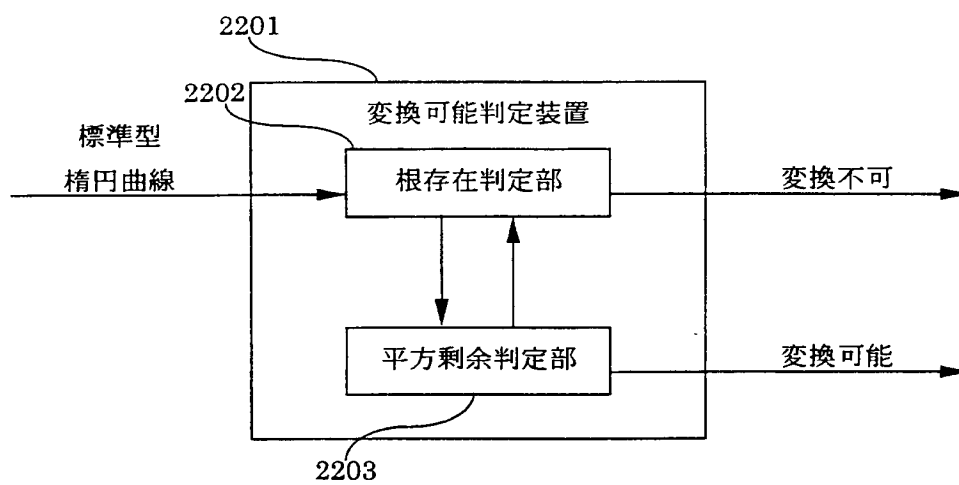
21/29

第 21 図



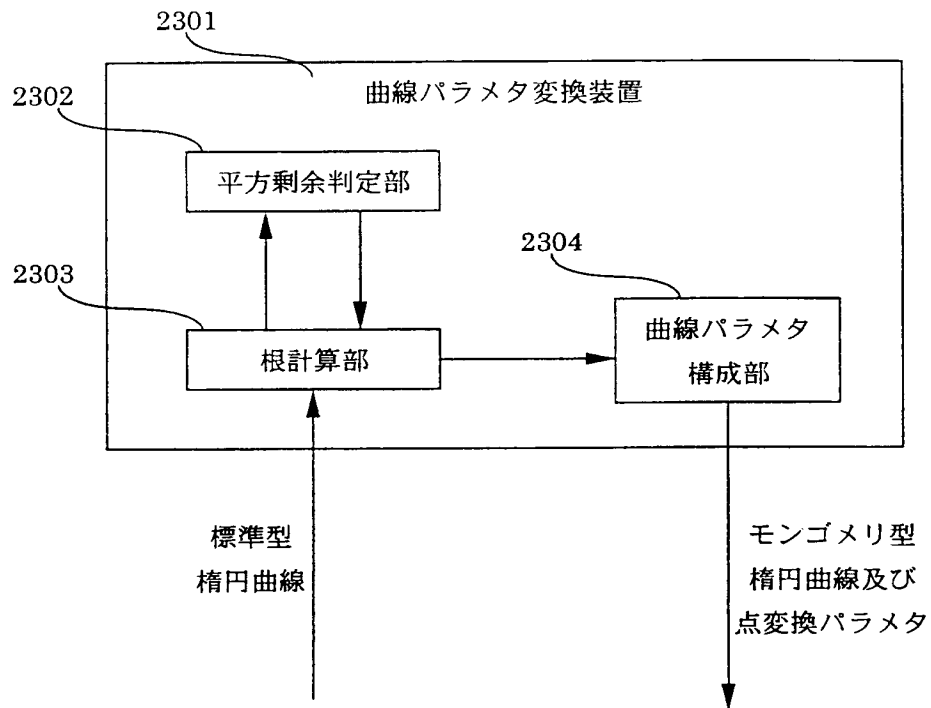
22/29

第 22 図



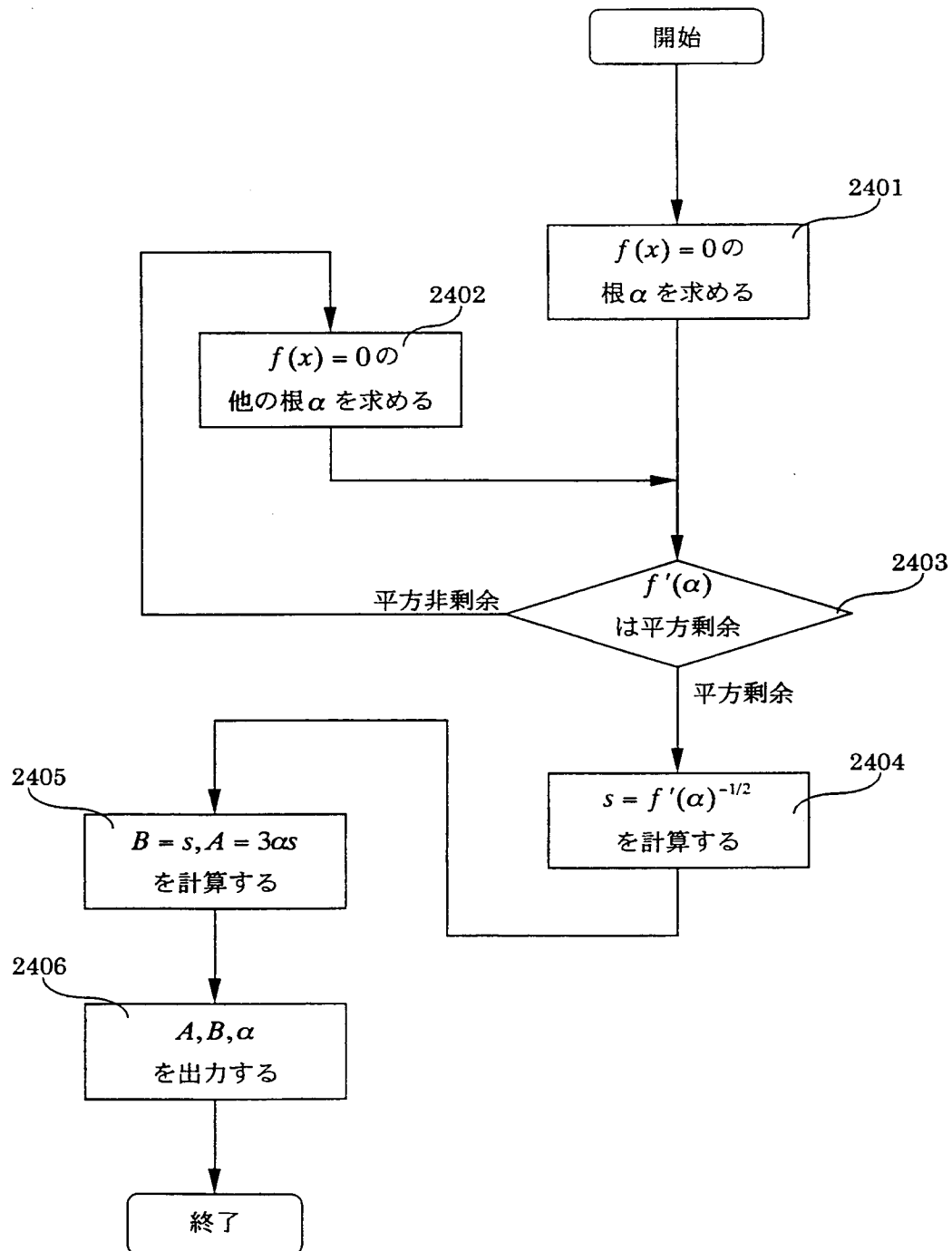
23/29

第 23 図



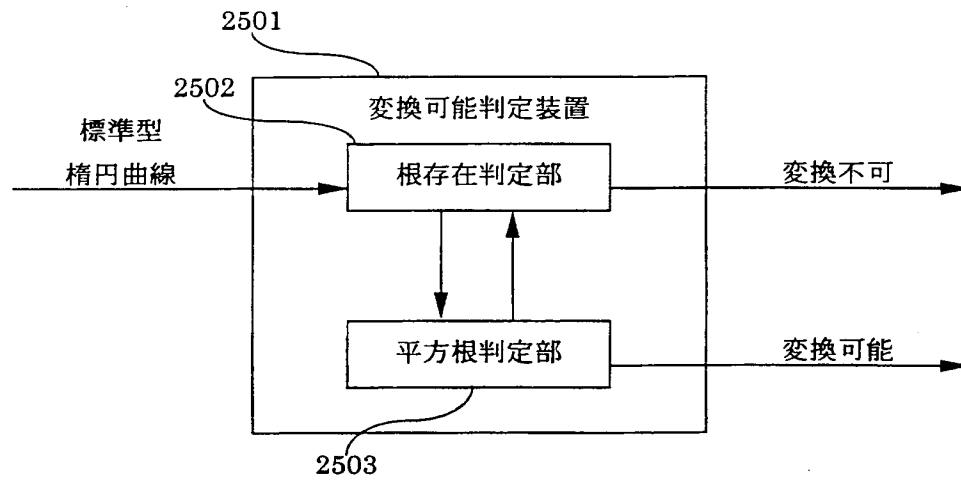
24/29

第 24 図



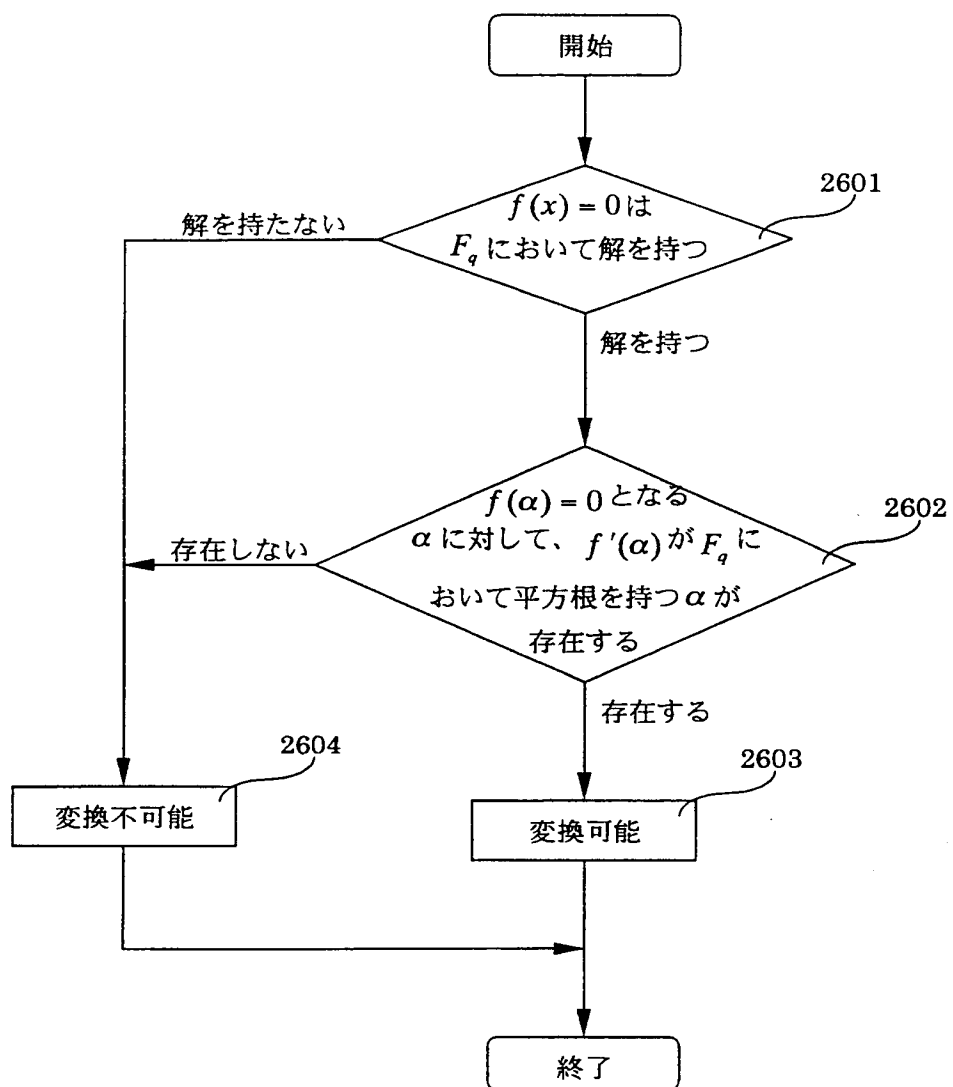
25/29

第 25 図



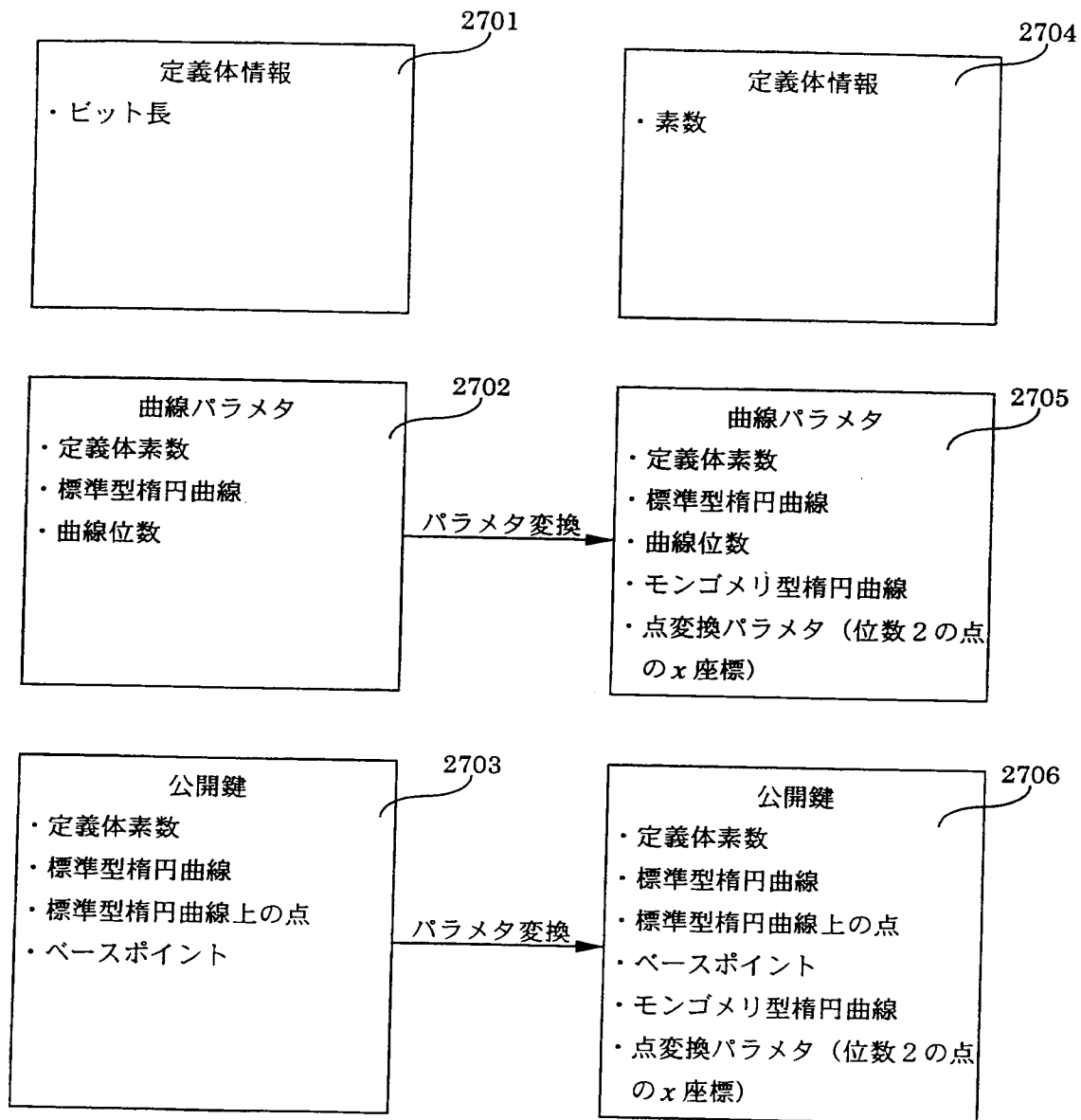
26/29

第 26 図



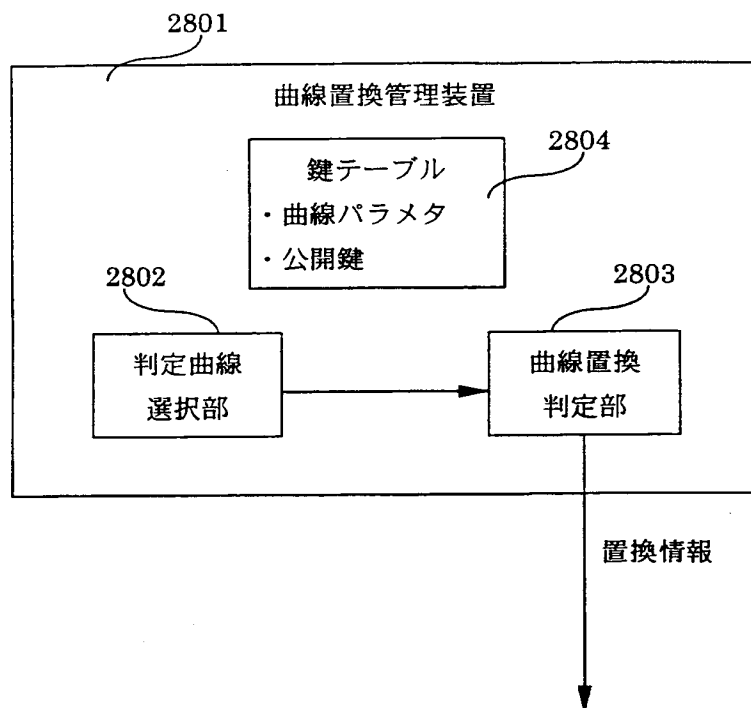
27/29

第 27 図



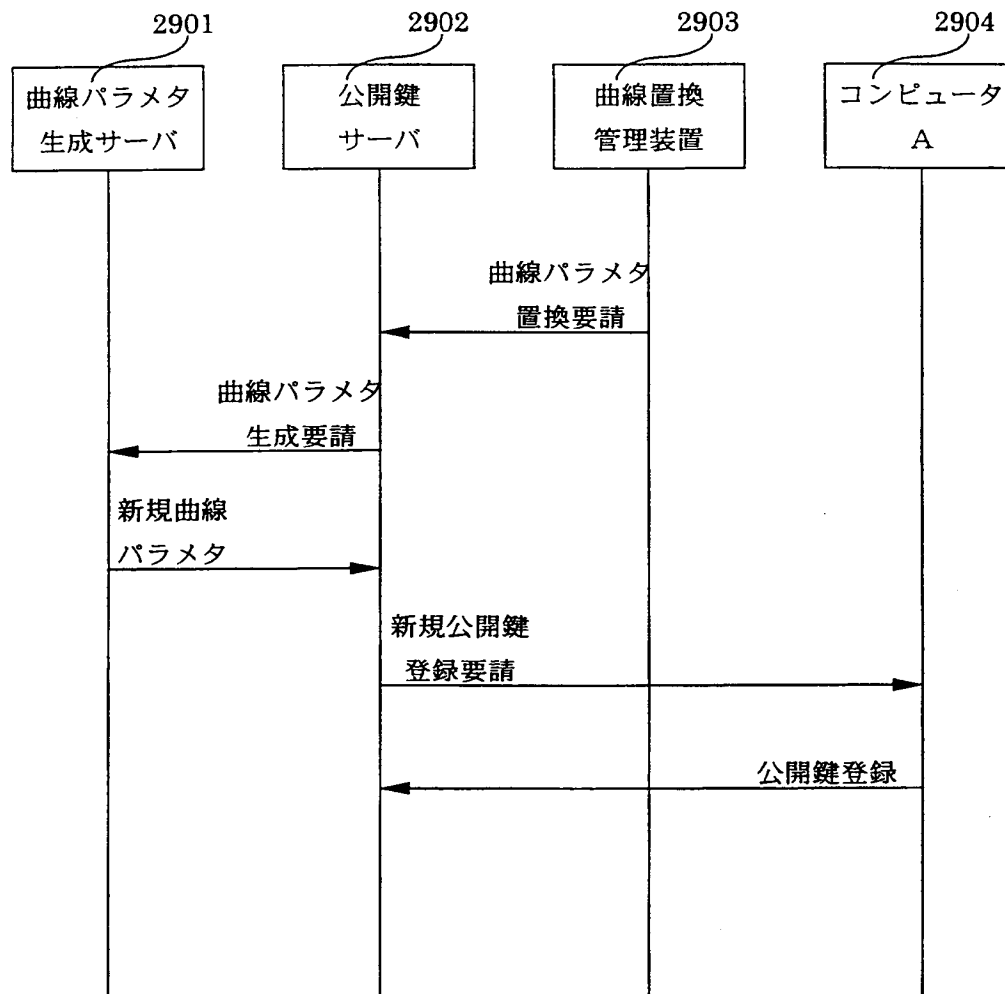
28/29

第 28 図



29/29

第 29 図



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/04869

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁶ G09C 1/00
H04L 9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁶ G09C 1/00 - 5/00, H04K 1/00 - 3/00,
H04L 9/00 - 9/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE (JOIS)
INSPEC (DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	Tetsuya IZU, "Daen Kyokusen Angou Enzan no Keisanhou ni tsuite", 1999 nen Angou to Joho Security Symposium Yokoushuu, (26 January, 1999), pp.275-280	12, 14, 15 9 10, 11
X Y A	Tetsuya IZU, "y Zahyou wo mochiinai Daen Kyokusen Enzan ni tsuite", Technical Research Report, the Institute of Electronics, Information and Communication Engineers, Vol.98, No.657, (10 March, 1999), pp.93-98 (SST98-129)	12, 14, 15 9 10, 11
Y	Kouichiro Akiyama, "Kakuteiteki Sosuu Hantei wo mochiita Daen Kyokusen Angou no Kagi Seisei", 1999 nen Angou to Joho Security Symposium Yokoushuu, (26 January, 1999), pp.773-778	9
Y	Tetsuya IZU, et al., "Anzena Daen Kyokusen Angou Parameter Sekkei (Hyoussuu 2nobawai)", 1999 nen Angou to Joho Security Symposium Yokoushuu, (26 January, 1999), pp.779-784	9
Y	Keiji Horiuchi, et al., "Daen Kyokusen no Kousei to sono Keisanryou Hyouka ni tsuite", Technical Research Report, the Institute of Electronics, Information and Communication Engineers, Vol.98, No.228,	9



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search
07 December, 1999 (07.12.99)

Date of mailing of the international search report
21 December, 1999 (21.12.99)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/04869

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 1-8,13
because they relate to subject matter not required to be searched by this Authority, namely:

Since subject matters in claims 1 to 8, 13 relate to merely mathematical theories or computer programs involving the conversion of an elliptic curve and the features of an elliptic curve, no international search is required.
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Subject matters in claims 9, 10 and 11 relate to an elliptic curve generating device which is used to generate an elliptic curve satisfying preset conditions.

Whereas, subject matters in claims 12, 14 and 15 relate to a so-called elliptic encryption; since an elliptic curve used in the encryption is a standard elliptic curve convertible into a Montgomery elliptic curve but a standard elliptic curve capable of such conversion is still at a prior art level, the subject elliptic curve constitute no special technical matter.

Therefore, claims 9, 10 and 11 and claims 12, 14 and 15 are not considered as satisfying a requirement of unity of invention.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/04869

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	(31 July, 1998), pp.31-36 (ISEC98-24)	
A	Kiyoshi Okishi, et al., "Daen Angou no Kousoku Shori ni kansuru 2, 3 no Kousatsu", Technucal Research Report, the Institute of Electronics, Information and Communication Engineers, Vol.98, No.228, (31 July, 1998), pp.37-42 (ISEC98-25)	9-12, 14, 15
A	Montgomery, P. L., "Speeding the Pollard and Elliptic Curve Methods of Factorization," Mathematics of Computation, Vol.48, No.177, (1987), pp.243-264	9-12, 14, 15

A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int. Cl. ⁶ G 0 9 C 1 / 0 0 H 0 4 L 9 / 3 0		
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int. Cl. ⁶ G 0 9 C 1 / 0 0 - 5 / 0 0, H 0 4 K 1 / 0 0 - 3 / 0 0, H 0 4 L 9 / 0 0 - 9 / 3 8		
最小限資料以外の資料で調査を行った分野に含まれるもの		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語) J I C S T ファイル (J O I S) I N S P E C (D I A L O G)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y A	伊豆哲也 “楕円曲線暗号演算の計算法について” 1999年暗号と情報セキュリティシンポジウム予稿集, (1999年1月26日), pp. 275-280	12, 14, 15 9 10, 11
X Y A	伊豆哲也 “y 座標を用いない楕円曲線演算について” 電子情報通信学会技術研究報告, Vol. 98, No. 657, (1999年3月10日), pp. 93-98 (SST98-129)	12, 14, 15 9 10, 11
Y	秋山浩一郎 “確定的素数判定を用いた楕円曲線暗号の鍵生成” 1999年暗号と情報セキュリティシンポジウム予稿集, (1999年1月26日), pp. 773-778	9
<input checked="" type="checkbox"/> C 欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日 07. 12. 99	国際調査報告の発送日 2.99	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 丸山 高政 5W 9570 電話番号 03-3581-1101 内線 3576	

第Ⅰ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT 17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☒ 請求の範囲 1-8, 13 は、この国際調査機関が調査することを要しない対象に係るものである。つまり、
請求の範囲 1-8, 13 に記載されたものは、楕円曲線の変換と楕円曲線の性質に関する数学の理論又はコンピュータプログラムにすぎないものであるから、国際調査をすることを要しない。
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であって PCT 規則 6.4(a) の第2文及び第3文の規定に従って記載されていない。

第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲 9、10 及び 11 は、楕円曲線生成装置に関するものであり、所定の条件を満たす楕円曲線を生成するためのものである。

一方、請求の範囲 12、14 及び 15 は、いわゆる楕円暗号に関するものであり、そこで使用される楕円曲線はモンゴメリ型楕円曲線に変換可能な標準型楕円曲線であるが、このような変換が可能な標準型楕円曲線は先行技術の域をでないから、この楕円曲線は特別な技術的事項ではない。

したがって、請求の範囲 9、10 及び 11 と請求の範囲 12、14 及び 15 は単一性の要件を満たしているとは認められない。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	伊豆哲也, 小暮淳, 野呂正行, 横山和弘 “安全な楕円曲線暗号パラメータ設計 (標数2の場合)” 1999年暗号と情報セキュリティシンポジウム予稿集, (1999年1月26日), pp. 779-784	9
Y	堀内啓次, 布田裕一, 境隆一, 笠原正雄 “楕円曲線の構成とその計算量評価について” 電子情報通信学会技術研究報告, Vol. 98, No. 228, (1998年7月31日), pp. 31-36 (ISEC98-24)	9
A	大岸聖史, 境隆一, 笠原正雄 “楕円暗号の高速処理に関する二, 三の考察” 電子情報通信学会技術研究報告, Vol. 98, No. 228, (1998年7月31日), pp. 37-42 (ISEC98-25)	9-12, 14, 15
A	Montgomery, P. L., “Speeding the Pollard and Elliptic Curve Methods of Factorization,” Mathematics of Computation, Vol. 48, No. 177, (1987), pp. 243-264	9-12, 14, 15